مدرسة وودلم بارك الخاصة
Woodlem Park School Private

Whole School Policy; E- Safety

Approved By:	**Dr. Prema Muralidhar**
Date of Review:	April 2022
Next Review Date:	April 2023

Introduction

We, The Woodlem Park School believes that online safety is an essential element of safeguarding children and young people in the digital world and especially in the distance learning. Internet and information communication technologies are an integral part of their world of education. Hence, to promote effective learning, Children and young people should always have an entitlement to safe internet access . So, it is our responsibility to educate our students on e-safety issues and to promote the acceptable behaviors among them. Children should be able to learn how to manage and respond to online risks. 'The whole school policy; E-safety' of The Woodlem Park School demonstrates safe and secure digital practices for the staff, students, and parents.

This Whole school policy describes the policies and practices of The Woodlem Park School, Ajman, related to the safety and security of the whole school community. Including the procedures, the school has to take to ensure the safety and security of the beneficiaries. The Woodlem Park School, Ajman, amended the existing policies of the school related to child safeguarding and protection to provide children with the safest learning environment in this distance learning mode.

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. This policy will be in effective from 15th September 2020.

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 cross-references 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. This policy will be in effective from 11th April 2022.

Definitions

safety	e safe 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	ople who visit school for a reason for required and essential service in collaboration.
The whole School community	fers 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	fers to the Network technology which is used by the people for information and communication
Social Media	fers to websites/ computer programs used by people to communicate or share information 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	fers 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.

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 responding 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 software 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

E. 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.

F. 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.

G. 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.

H. 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.

I. 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 account of any emerging issues and technologies.

Policy Statements

1) Infrastructure

All users of WPS computer networks have clearly defined access rights, enforced using a username and password login system. Account privileges are achieved through the file and folder permissions and are based upon each user's requirements. Pupils' accounts are restricted and do not allow access to all network drives. Guests are required to login using a visitor login that has limited network access.

A permanently enabled filtering system is used to filter inappropriate material. Additionally, web pages are scanned for content as requested. Any changes to setting must be requested through the WPS IT Helpdesk. All changes made to Internet filtering are logged. Security software is installed on all computers.

Staff should be aware that Internet traffic is monitored and can be traced to the individual user. It is the responsibility of the user to ensure that they have logged off the system when they have completed their task and to keep their user credentials confidential.

Please refer to the WPS IT Acceptable Use Policy for further details.

Rules for publishing material online (including images of pupils)

Websites are a valuable tool for sharing information and promoting pupils' and students' achievements. We recognize the potential for abuse. Therefore, the following principles will always be considered:

- If an image, video or audio recording of a pupil/student is used, their surname should not be used (including in credits).
- Staff **must not** take photographs of pupils or students using their personal devices
- All pupil/student photographs must be taken using WPS equipment.
- Files should be appropriately named in accordance with these principles.
- Only images of pupils/students in suitable dress should be used and group photographs are preferred (though not exclusively) in preference to individual Photographs.
- Parents/care givers are given the opportunity to withdraw the permission to publish images/audio/video of their child on the website.
- Content should not infringe the intellectual property rights of others – copyright may apply to text, images, music or video that originate from other sources.
- All copied or embedded content should be properly referenced.

- Content should be polite and respect others.
- Material should be proofread by a member of the 's Senior Leadership Team before being published.
- Children and young people use a variety of online tools for educational purposes. They will be asked to only use their first name or a suitable avatar for any work that will be publicly accessible and will be required to follow the principles listed above before sending any work for publishing. Staff should encourage contributions that are worthwhile and develop a discussion topic.

When photos and videos of events are permitted to be taken by parents and care givers, they will be asked not to publish them on any public area of the Internet, including social networking sites.

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 WPS.

- 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 WPS IT Acceptable Use Policy.

2) Education and Training

The aim of e-safety education within WPS 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, LMS and/or newsletters) 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

WPS 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 WPS 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 WPS 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 WPS systems.

Data Protection

Staff must ensure that they:

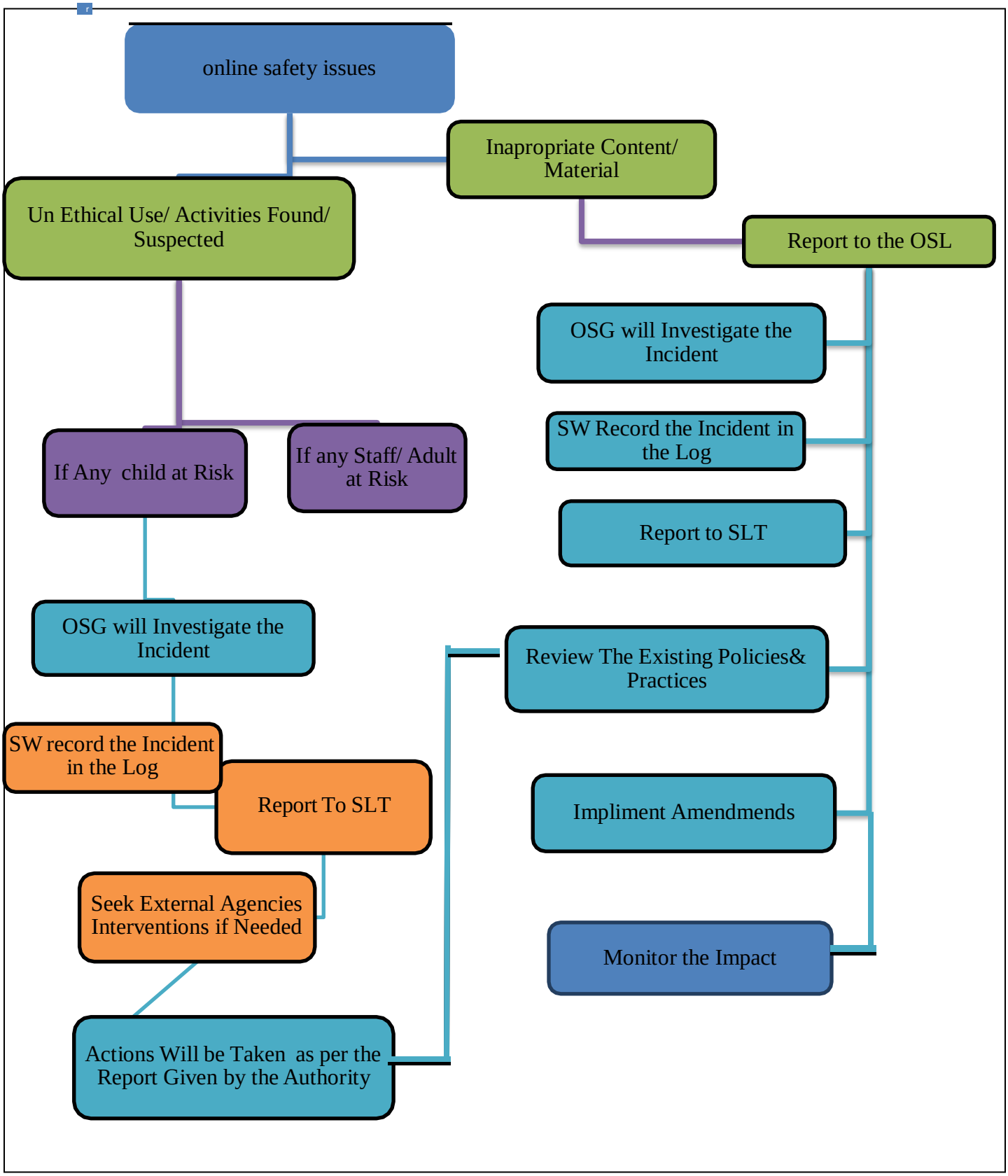
- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse;
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' or 'locked' at the end of any session in which they are using 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 organisation e.g. as part of a safeguarding investigation. **WPS 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.

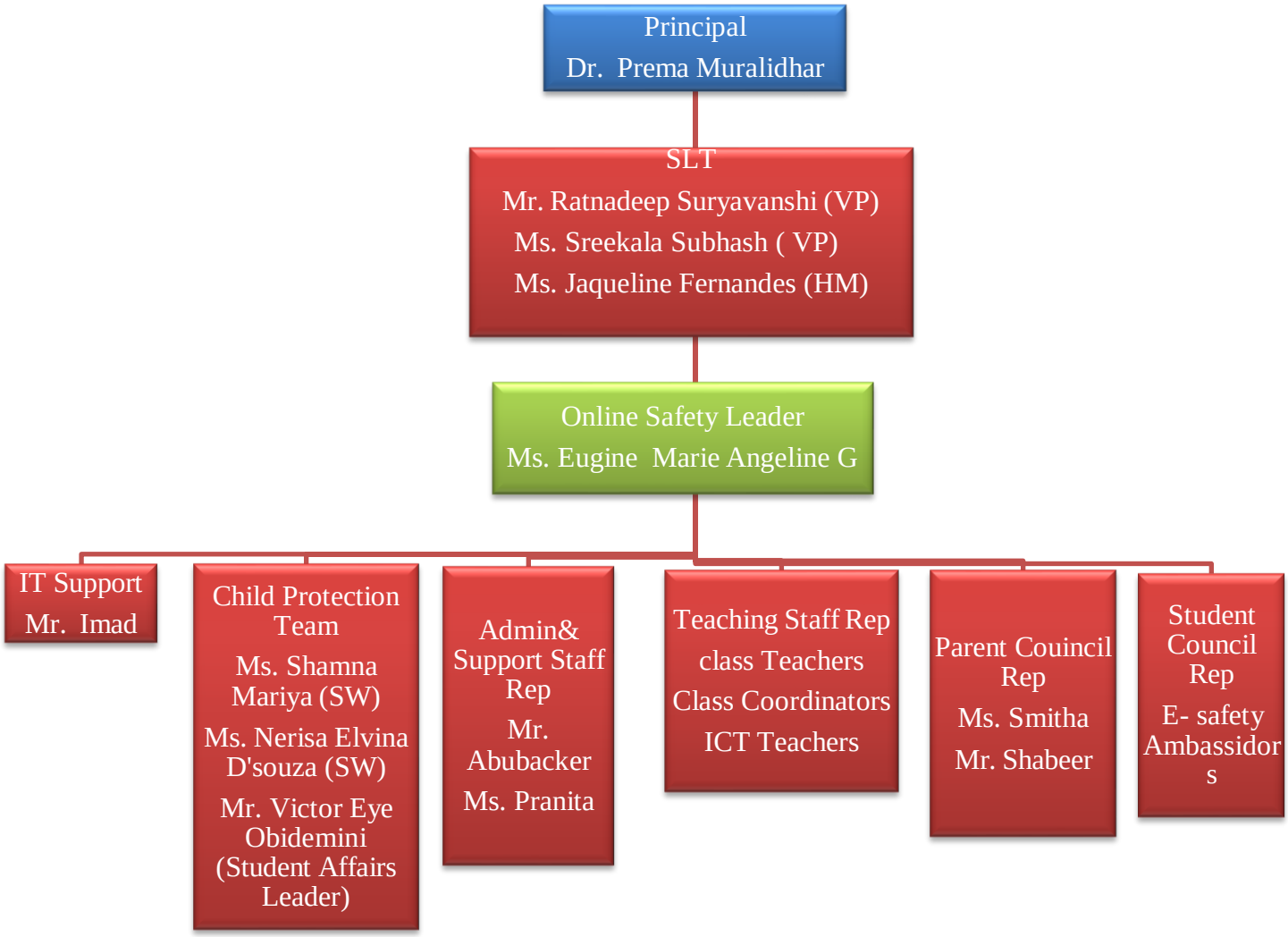
3) Responding to incidents:

This guidance is intended for use when the whole school community need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Procedure


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

Structure of Online Safety Group



Cross Reference

- The child Protection & Safeguarding Policy of WPS
- School Health& Safety Policy
- Acceptable Use Policy
- Social Media Policy
- Electronic Communication 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 in distance learning 2020
- UAE's Federal Law 5 of 2012
- UAE's Federal Law 12 of 2016
- UAE's Federal Law 34 of 2021

Acceptable Use Policy

Overview

This Acceptable Use Policy sets out responsibilities, procedures, and protocols that must be followed by the beneficiaries of WPS to encourage the safe, secure, and appropriate use of the all-digital and communication technologies by the stakeholders of WPS, including the use of school-based devices, the internet, email, instant messaging, social networking sites, games and other electronic devices etc. .

This policy applies to all the stakeholders of Woodlem Park School, including parents, students, staff, all personnel affiliated with third parties, including vendors and visitors. This policy applies to all equipment that is owned or leased by Woodlem Park School.

Links to other policies:

This policy has cross reference to other school policies, including child protection and safeguarding Policy, Student behavior Management Policy and other relevant policies as mentioned in the school E safety policy like social media policy, mobile device policy, and password policy etc.

Objectives:

- To create awareness among students on appropriate and acceptable use of all online technologies to enable them to protect themselves from online safety threats/ issues.
- To outline the roles and responsibilities of all stakeholders
- To create awareness among all stakeholders on the procedures and protocols to be followed by them to deal with online safety issues.

While Woodlem Park School's IT Department desires to provide a reasonable level of freedom and privacy, users should be aware that all Woodlem Park School-owned equipment, network infrastructure, and software applications are the property of Woodlem Park School and therefore are to be used for official use only. Also, all data residing on Woodlem Park School-owned equipment is also the property of Woodlem Park School and therefore, should be treated as such, and protected from unauthorized access.

General instructions to the stakeholders

Acceptable use:

- All use of the Internet must be in support of educational and research objectives consistent with the mission and objectives of the WPS.

- Proper codes of conduct in electronic communication must be used. When using e-mail, extreme caution must always be taken in revealing any information of a personal nature.
- All passwords used to access Woodlem Park School systems must be kept secure and protected from unauthorized use.
- No user account can be shared between individuals. Authorized users are responsible for the security of their own passwords and accounts.
- Do not transfer personally identifiable information on portable equipment and storage devices.
- All computers residing on the internal Woodlem Park School network, whether owned by the employee or Woodlem Park School, shall be continually executing approved virus-scanning software with a current, up-to- date virus database.
- Users must use extreme caution when opening e-mail attachments received from unknown senders.
- All workstations should be kept secure. Users should lock the workstation when not attended to protect unauthorized users from accessing secure files.
- From time to time, the WPS will make determinations on whether specific uses of the network are consistent with the acceptable use practice.

Unacceptable Use:

Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Woodlem Park School.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Woodlem Park School or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server environments (e.g., viruses, worms, Trojan horses, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work/ learning is being done at home.
- Using a Woodlem Park School computing asset to actively engage in procuring or transmitting

material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

- Making fraudulent offers or services originating from any Woodlem Park School account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to the Woodlem Park School IT Department is made.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or IMs, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Use of unsolicited mail originating from within Woodlem Park School's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Woodlem Park School or connected via Woodlem Park School's network.

Responsibilities:

Staff:

- Ensure that students are protected and supported in their use of online technologies, and that they know how to use them in a safe and responsible manner.
- Use ICT equipment safely and correctly and be responsible for the management of the equipment within their teaching space.
- Protect confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they are logged on
- Follow the procedures of reporting if any issues/ threats identified (refer reporting flow chart)
- Report accidental access to inappropriate materials to the IT Supporter so that the site(s) is/are added to the restricted list.

- Public postings by employees from a Woodlem Park School email address should contain the following disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Woodlem Park School, unless the posting is during business duties:

Any views or opinions presented in this message are solely those of the author and do not necessarily represent those of Woodlem Park School. Employees of Woodlem Park School are expressly required not to make defamatory statements and not to infringe or authorize any infringement of copyright or any other legal right by electronic communications. Any such communication is contrary to Woodlem Park School policy and outside the scope of the employment of the individual concerned. Woodlem Park School will not accept any liability in respect of such communication, and the employee responsible will be personally liable for any damages or other liability arising.

- Provide suggestions/ information on any new or arising issues and risks that may need to be included within policies and procedures or any e-safety incidents
- Under no circumstances is an employee of Woodlem Park School authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Woodlem Park School-owned resources.

Students:

- Responsible for following the Acceptable Use Agreement whilst within school as agreed each academic year or whenever a new student starts at the school for the first time.
- Involve in the review of school Acceptable Use Policy. Provide suggestions/ information on any new or arising issues and risks that may need to be included within policies and procedures or any e-safety incidents.
- Report accidental access to inappropriate materials to the IT Supporter so that the site(s) is/are added to the restricted list.
- Follow the procedures of reporting if any issues/ threats identified or experienced (refer reporting flow chart).

Guidelines for students

- Use the electronic resources, including storage space, only for educational purposes related to work in Woodlem Park School, and not for any personal, commercial or illegal purposes.
- Use the Internet only with the permission/ supervision of the staff member in charge.
- Shall not use games or other electronic resources that have objectionable content or that engage student/s in an inappropriate simulated activity.
- Shall not disclose password to any other user, nor attempt to learn or to use anyone else's password, and shall not transmit any personal or confidential information about yourself or others.

- Shall not upload, link, or embed an image of yourself or others to non-secured, public sites without the permission of school authority and a signed parental consent.
- Shall not engage in the activities related to Cyberbullying, including make statements or use the likeness of another person through website postings, email, instant messages, etc., that harass, intimidate, threaten, insult, libel or ridicule students or staff of the school community, make statements that are falsely attributed to others, or use language that is obscene.
- Do not attempt to access, upload, or transmit material that attacks ethnic, religious or racial groups, or material that is pornographic or explicitly sexual in nature.
- Do not violate copyright laws, damage or tamper with hardware or software, vandalize or destroy data, intrude upon, alter or destroy the files of another user, introduce or use computer "viruses," attempt to gain access to restricted information or networks, or block, intercept or interfere with any email or electronic communications by staff to parents, or others.
- Shall not use, or create for others, any program to interfere with, change, or interact with programs, security settings, systems, or devices that are the property of the Woodlem Park School and are used for school-related purposes by students, parents and staff.
- Shall not imply, directly or indirectly, either publicly or privately that any program or "app" you create is associated with or a product of the Woodlem Park School, or shall not use any Woodlem Park School logos or images directly or indirectly to associate with any such program.
- Shall understand that the prohibited conduct described above is also prohibited off campus when using private equipment if it has the effect of seriously interfering with the educational process, and that such off-campus violations may lead to disciplinary measures.

Parents:

- Ensure that students are protected and supported in their use of online technologies, and that they know how to use them in a safe and responsible manner.
- Familiarize with the other relevant policies of the school related to E- safety. so that in the event of misuse or a threat, the correct procedures can be followed.
- Educate children on appropriate and inappropriate use of technologies and thereby enable them to use technologies in a responsible way.
- Follow the procedures of reporting if any issues/ threats identified or experienced (refer reporting flow chart).

Guidelines for Parents:

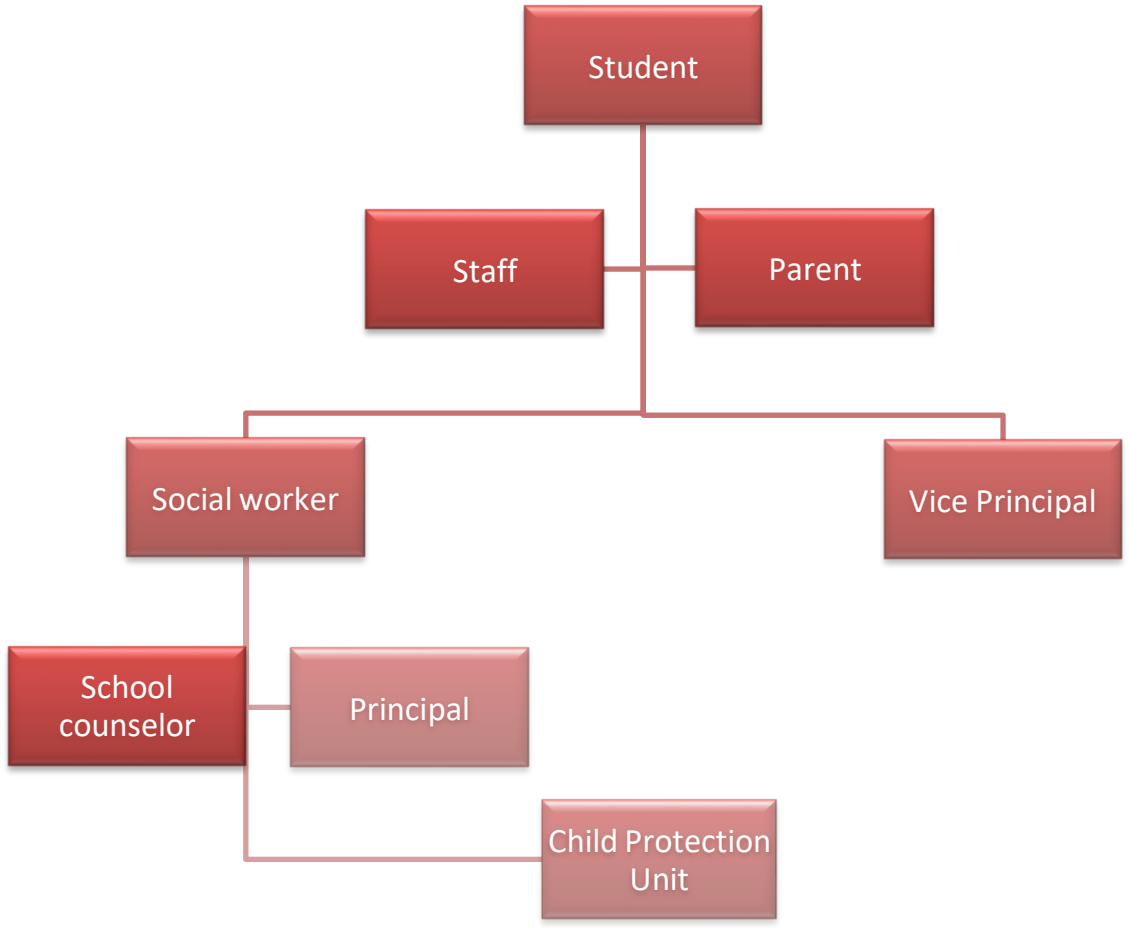
- Do not allow your child to use electronic devices/ internet from his/ her private areas. Always instruct them to use devices in a room that is easily accessible to all family members.
- Get to know the computer services your child uses. Check your child's online activities on regular basis.

- Do not allow your child to arrange a face-to-face meeting with an online user who is unknown to you.
- Set reasonable rules and guidelines for computer use by your children. Monitor their compliance with these rules, especially when it comes to the amount of time your children spend on the computer. A child or teenager's excessive use of online services or bulletin boards, especially late at night, may be a clue that there is a potential problem.
- Encourage your children to report immediately to you if, they experience any online threats/ issues.

Procedure

- Follow the referral procedure when any violations of the AUP identified or experienced
- The school Online Safety Group will investigate the issue.
- If any child found guilty, the school will deal the issue with the provisions mentioned in the **'The student behavior management policy no: 851 of year 2018' and 'Students' behavior Management in distance learning 2020 2021 and by the provisions 'U A E Government's 'Federal laws.**
- If any adult found guilty, the school will move with necessary legal/ disciplinary actions against the person.

Referral process Flow Chart



AUP Agreement Form

Student

I …… Of Grade…… hereby acknowledge that I have read the 'The acceptable use policy', of the school. I agree to follow the rules contained in this policy on the use of the Technologies, Internet resources and electronic devices. I will use the Internet, electronic devices and Technologies in a responsible way and obey all the rules explained to me by the School.

I understand that I must face disciplinary actions mentioned within 'The Ministerial Resolution No.851 of Year 2018 on Code of Behavior Management for Students in the General Education Institutions Students' Behavior Management in Distance Learning 2020- 2021' if I do not behave appropriately.

Signature:

Parent or Guardian

As a parent or guardian of this student, I have discussed the standards with my child and understand that misuse of the school's Network, Internet access, and Technology resources will result in termination of all In ternet and Technology privileges for my child and possibly lead to disciplinary actions.

Parent Name:

Parent Signature: Date:

Visitors:

Visitors and contractors are asked to sign this document before they are allowed get access to the school-owned devices, networks, or other technology/s.

1. I understand that any activity on a school device or using school networks/platforms/internet may be captured by one of the school's systems security, monitoring and filtering systems and/or viewed by an appropriate member of staff.
2. I will leave my phone in my pocket and turned off. Under no circumstances will I use it (or other capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils/students. If required (e.g. to take photos of equipment or buildings), I will have the prior permission of the headteacher (this may be delegated to other staff) and it will be done in the presence of a member staff.
3. If I am given access to school-owned devices, networks, cloud platforms or other technology:
    - I will use them exclusively for the purposes to which they have been assigned to me, and not for any personal use
    - I will not attempt to access any pupil / staff / general school data unless expressly instructed to do so as part of my role
    - I will not attempt to contact any pupils/students or to gain any contact details under any circumstances
    - I will protect my username/password and notify the school of any concerns
    - I will abide by the terms of the school Data Protection Policy [refer Data Protection Policy]
4. I will not share any information about the school or members of its community that I gain as a result of my visit in any way or on any platform except where relevant to the purpose of my visit and agreed in advance with the school.
5. I will not reveal any new information on social media or in private which shows the school in a bad light or could be perceived to do so.
6. I will only use any technology during my visit, whether provided by the school or my personal/work devices, including offline or using mobile data, for professional purposes and/or those linked to my visit and agreed in advance. I will not view material which is or could be perceived to be inappropriate for children or an educational setting.

To be completed by the visitor/contractor:

I have read, understood and agreed to this policy.

Signature/s: _____

Name: _____

Organization: _____

Visiting / accompanied by: _____

Date / time: _____

To be completed by the school (only when exceptions apply):

Exceptions to the above policy: _____

Name / role / date / time: _____

Acceptable Use Policy Agreement: Staff

I hereby agree to abide by all the points mentioned in the Acceptable Use Policy. I understand that I must use school ICT systems and equipment in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognize the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people. I understand that it is my responsibility to ensure that I read and understand the school's most recent e-safety policies and remain up-to-date.

Name ……..

Signature …… Date ……..

Child Safety Policy

I ntroduction

Ministry of Education (MoE) launched a 'Child Protection Unit' initiative for the benefit of students of government and private schools across the UAE. The initiative is aimed at protecting children from all forms of harm, negligence, and abuse, which they may experience at school or home and maintaining their safety with regard to their physical, psychological, and educational aspects. We, The Woodlem Park School Ajman, believe that all children have a right to be safe, protected from abuse, and able to reach their full potential. We recognize that all staff and governors have a full and active part to play in protecting our pupils from harm and that the child's welfare is our paramount concern.

The policy is intended to provide clear direction for all the stakeholders to support the school's commitment to best practice and appropriate procedures to ensure that child protection concerns are handled sensitively and professionally.

Definitions

Student	Each learner enrolled at Woodlem Park School Ajman, including those ~~p~~people of determination and those of special needs.
Parents	Refers to birth parents and other adults who are in a parenting role.
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.
Staff	Refers to all those working for or on behalf of the school, full time or part time.
Bullying	Shall mean any form of intentional psychological, physical, Verbal, electronic or digital abuse, or intimidation, or menace conducted by a student or a group of students

	against one student or more, or against the school staff, on frequent basis.
Sexual harassment	Shall mean any word or act that suggests or has symbolic sexual connotations made by a student or staff, whether verbally, by writing, by physical contact, by looking, by eye winking, by showing sensitive parts of the body…etc.
Sexual assault	Shall mean committing any sexual act against a child, juvenile or an adult, including sexual intercourse, whether with or without the victim's consent.
Cyberbullying	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 he religious values.
C P T	**Child Protection Team** is one of the school management committees, which is concerned with discussing the students' issues, in protection and safeguarding and taking the proper decision in this regard, in accordance with the provisionsof child rights law of U A E.

Objectives

- To create awareness among the stakeholders on 'the various initiatives of U A E for the protection of children including; federal law no: 3 of 2016 (Wadeema's Law), child protection unit, federal law no: 5 of 2012 on combatting cybercrimes etc.
- To provide all staff and parents with the necessary information to enable them to meet their statutory responsibilities to promote and safeguard the wellbeing of children.

- To ensure that appropriate action is taken where it is alleged that a child is suspected of being abused, or is actually being abused.
- To demonstrate the school's commitment with regard to safeguarding children.

Roles & Responsibilities

Staff

- All staff are equally responsible to identify concerns early, provide help for children, and prevent concerns from escalating.
- Inform the social worker and the vice principal/headmistress if any form of child abuse is suspected or reported.
- Keep written records of concerns, even where there is lack of evidence (records should state facts not opinions).
- Respect the confidentiality of all concerned regarding the welfare of children. Keeping the confidentiality of the matter is mandatory.
- Integrate child protection issues into relevant teaching and learning to create awareness among children.
- Staff should follow the referral process(detailed in page no: 6)

Staff must not:

- Question children.
- Suggest alternatives to what a child has said.
- Get the child to write about, or depict their experience in some other way.
- Reporting to the parents directly especially in the case of sensitive issues.
- Question potential witnesses.
- Conduct medical examinations.
- Delay referral/ No Referral

Social Worker

- The provision of training, advice and support to staff.
- Maintaining accurate and secure child protection records.

- Coordinate with the school counselor to provide psycho- social support to the child.
- Monitoring the changes and development of children who are at risk.
- In consultation with the principal and vice principal refer alleged cases of child abuse to the Child Protection Unit.

Parents

If your child report any type of abuse or bullying:

- Do not panic. Be as calm and natural as possible.
- Assure support to the child. Listen to what the child has to say. Give them the time and opportunity to tell as much as they are able and wish to.
- Report to the school immediately.
- Collaborate with the school'sChild protection Team for further procedures.

Child protection Team

- Develop and implement policies and programs to ensure the protection and safeguarding of students.
- Meet periodically to evaluate policy plans and amend accordingly.
- Support staff to establish a safe environment for the students.
- Liaise with the child protection unit for getting updates amendments on U A E's child protection laws. And conduct awareness campaigns accordingly.

Cyberbullying

Cyberbullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group which intended to harm others. It can take numerous forms; threats, intimidation, harassment, sexting, defamation, exclusion, impersonation, unauthorized publication of private information or images, and trolling, etc. It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target.

We The Woodlem Park School is using the provisions of U A E Government's 'Federal law no: 5 of 2012, 'The student behavior management policy no: 851 of year 2018' and 'Students' behavior

Management in distance learning 2020- 2021' to ensure the online safety of our students and to deal with the cyberbullying offenses.

Guidance for Students

If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, or a member of staff of the school.

- Students should follow the school's code of conduct and MoE's Students' behavior Management in distance learning 2020 2021.
- Do not answer abusive messages but save them and report them
- Do not delete anything until it has been shown to your parents/Guardians or a member of staff at school (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyber-bullying)
- Do not give out personal details or contact information without the permission of a parent/guardian (personal data)
- Be careful who you allow to become a friend online and think about what information you want them to see.
- Protect your password. Do not share it with anyone else and change it regularly
- Always log off from the computer when you have finished or if you leave the computer for any reason.
- Always put the privacy filters on to the sites you use. If you are not sure how to do this, ask a teacher or your parents.
- Never reply to abusive e-mails
- Never reply to someone you do not know
- The school will deal with cyberbullying in the same way as other bullying. Do not think that because it is online it is different to other forms of bullying.
- The school will deal with inappropriate use of technology in the same way as other types of inappropriate behavior and sanctions will be given in line with the MoE's Students' behavior Management in distance learning 2020- 2021.

Students must not:

Students may use the Internet only for learning related activities that are approved by a teacher. They must not cause interference or disruption to other people or equipment, and students may not access or distribute inappropriate material. This includes:

- Distributing spam messages or chain letters.
- Accessing or distributing malicious, offensive or harassing material, including jokes and images.
- Bullying, harassing, defaming or giving offence to other people.
- Spreading any form of malicious software (e.g. viruses, worms).
- Accessing files, information systems, communications, devices or resources without permission.
- Using for personal financial gain.
- Using non-approved file sharing technologies (e.g. Torrent).
- Using for non-educational related streaming audio or video.
- Using for religious or political lobbying.
- Downloading or sharing non-educational material.

Guidelines for Parents/ Guardians

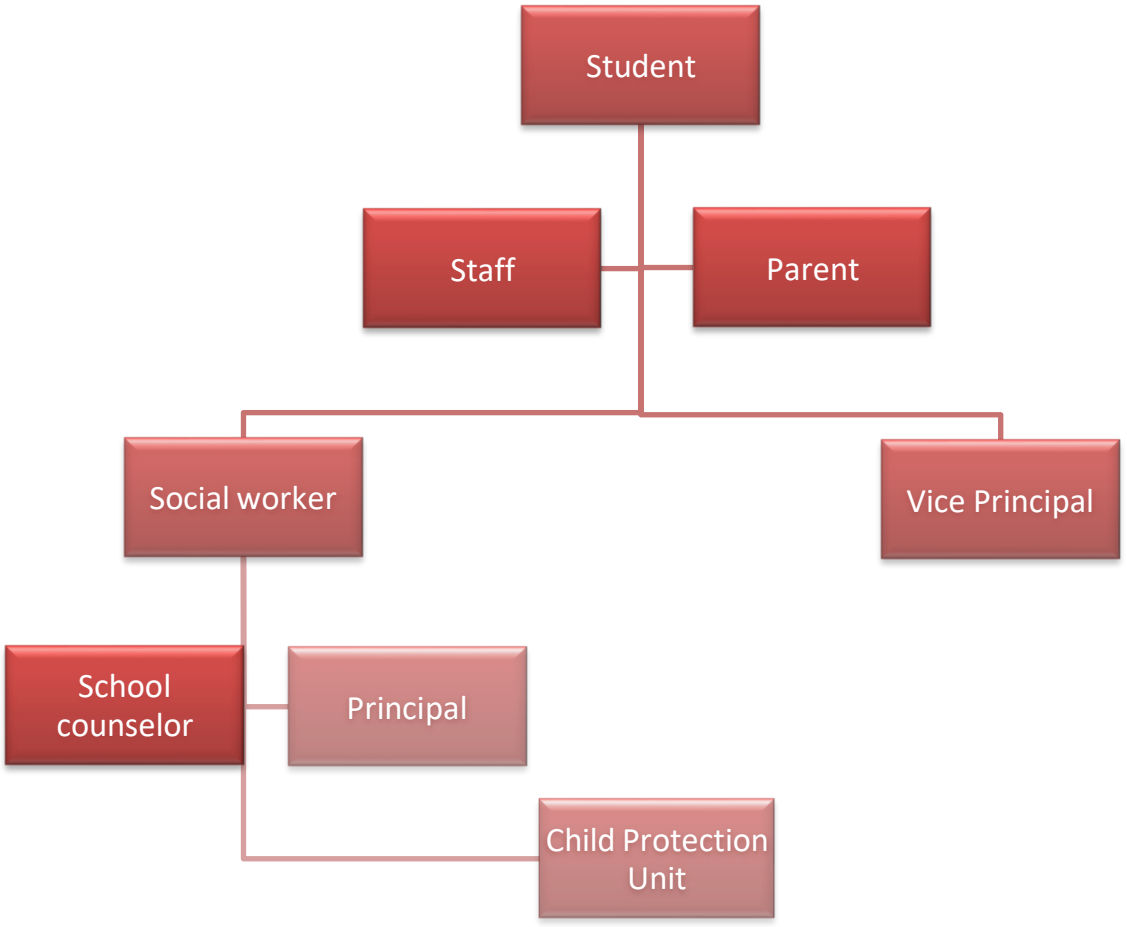
It is vital that parents/Guardians and the school work together to ensure that all students are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying.

Parents/

Guardians must play their role and take responsibility for monitoring their child's online life.

- Parents/ Guardians can help by making sure their child understands the school's policy and above all, how seriously the school takes incidents of cyber-bullying.
- Be aware of what your children are doing online.
- Ensure children are not using private areas for their online activities. Provide a space where parents can access easily.
- Parents/ Guardians should also explain to their children legal issues relating to cyber-bullying.
- If parents/ Guardians believe their child is the victim of cyber-bullying, they should save the offending material.
- Parents/ Guardians should contact the school social worker or section head as soon as possible.

Referral process Flow Chart



School procedure to deal with cyberbullying

- The teachers, parents, or students should report the incident to the responsible persons of the school immediately.
- The school Child Protection Team will investigate the issue.
- If any child found guilty, the school will move with the provisions mentioned in the **'U A E Government's 'Federal law no: 5 of 2012, 'The student behavior management policy no: 851 of year 2018' and 'Students' behavior Management in distance learning 2020 2021'**

Contact Information

SCHOOL			
Designated Person	**Name**	**Contact no:**	**Email**
Vice Principal (Admin)	MrRatnadeep	054 791 3869	vp.aa@woodlempark.ae
Headmistress (primary)	Ms Jacqueline	054 791 3867	wps.hm@woodlempark.ae
Social Worker:	MsShamnaMariya	055 9363554	Wps.bmc@woodlempark.ae

CHILD PROTECTION UNIT		
Contact no:	**Email**	**Hotline no:**
04- 217666	CPU@moe.gov.ae	116111

CYBERBULLYING			
	Contact no:	**Email**	**Hotline no:**
police	999	Hos.up@woodlempark.ae	116111
Ministry of Interiors	8002626	www.ecrime. ae	

Reference

- The Federal Decree Law No.5 of 2012, in respect of cybercrimes combat
- The Federal Law No.3 of 2016, in respect of the Law of Child's rights and protection (Wadeema's Law).
- Ministerial Resolution No.851 of Year 2018 on Code of Behavior Management for Students in the
- General Education Institutions
- Students' Behavior Management in Distance Learning 2020- 2021
- Ahmed Ashfaq; 10 February 2020; "One in three students, age 12 to 15 year, suffer from regular bullying worldwide"; Gulf News online.
- Robertson Fiona; January 2020; "Cyberbullying in the UAE: A Snapshot of Cyberbullying Laws in the UAE"; Al Tamimi& C0

Websites:

- www.tra.gov.ae; Telecommunications Regulatory Authority(T R A)
- www.moe.gov.ae; Ministry of Education; Child Protection Unit
- www.dubaipolice.gov.ae; Cyberbullying.

Mobile Device/ Own Device Policy

Overview

The policies, procedures and information within this document apply to all the mobile devices/ own devices used at the Woodlem Park School, including any other device considered by administration to come under this policy. Teachers may set additional requirements for use in their classrooms.

This policy will operate in connection to the School's acceptable use policy ,MoE's The student behavior management policy no: 851 of year 2018 and Students' behavior Management in distance learning 2020.

This policy is applicable to all Mobile devices and any wearable technology

While these are not school property, also fall under the Acceptable Use Policy whilst on school property or whilst on school related activities. However, the school is not responsible for the repairs,lossortheftoranydamage resultingfromtheiruse on schoolpropertyorduringschoolrelatedactivities. Improper use of the devices will lead to immediate confiscation and permanent denied access to the school Wi-Fi network. The devices will only be returned the parents or legal guardians of the student owning the device.

Using Mobile and own devices at School

Mobileandown devicesareintendedforuse at school each day. In addition to teacherexpectations for Mobile device and own device use, school messages, announcements, calendars and schedules may be accessed using the mobile device and own device. The mobile device or own device cannot be used unless a teacherhas given permission for its use.

Inappropriate content

Inappropriate material or photos are not to be stored on mobile device and own device. mobile device and own device containing material considered inappropriate by the school will be confiscated and returned only to a responsible adult. The device may not be brought to school until the offending material/Apps are removed.

Inspection

Students may be selected at random to provide their device for inspection including mobile device and own device to ensure that there are not any violations to this policy.

Acceptable Use

The use of School technology resource is a privilege, not a right. This policy is provided to make all users aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources. If a person violates any of the User Terms and Conditions named in this policy, privileges will be terminated, access to the school's technology resourceswillbedenied, BYODdevices will bedenied access to the school's network and Wi-Fi facilities and the appropriate disciplinary action shall be applied. 'The student behavior management policy no: 851 of year 2018' and 'Students' behavior Management in distance learning 2020' shall be applied to student infractions.

Responsibilities

Parent/Guardian

Parents have a responsibility to talk to their children about values and the standards that their children should follow regarding the use of the Internet as they would in relation to the use of all media information sourcessuch as television, telephones, movies, radio andsocial media.

Staff

- Educate students on appropriate and acceptable use of devices.
- Provide guidance to aid students in doing research and help assure student compliance of the acceptable usepolicy.
- Monitoring of students' behavior when they are using devices.
- Report or notify the SLT if any malpractices, issues, or threat found related to the students' use of devices.

Students

- Usingmobiledevicesinaresponsibleandethicalmanner.
- Obeying general school rules concerning behavior and communication that apply to Technology equipment use.
- Usingalltechnologyresources in anappropriatemanner.
- Helping the school protect our computer system/device by contacting an administrator about any securityproblemstheymay encounter.
- Monitoring all activity on their account(s).

This policy will operate in connection to the School's acceptable use policy,MoE's The student behavior management policy no: 851 of year 2018 and Students' behavior Management in distance learning 2020.

Woodlem Park School
...For a Sustainable Growth

Social Media Policy/Guideline

Overview:

The Woodlem Park School recognizes the rights of students, faculty, staff, and employees who want to participate in online social networking. Our guidelines are designed to create an atmosphere of good will, honesty, and individual accountability. Woodlem Park students, faculty, and staff should always keep in mind that information produced, shared, and retrieved by them is a reflection on the school community and is subject to the School's policies. When accessing, creating, or contributing to any blogs, wikis, podcasts, or other social media for classroom or, in most cases, for personal use, we expect you to keep these guidelines in mind. Failure to meet or follow these guidelines may result in disciplinary action.

Students: Social Media Guidelines:

In accordance with code of conduct, we expect Woodlem Park Students to set and maintain high ethical standards in their use of social networking. Since social media reaches audiences far beyond the community, students must use social sites responsibly and be accountable for their actions. If a student sees anything of concern on a fellow Woodlem Park student's social networking page or account, they should immediately contact the Principal, the Manager of Information Technology, or another adult within the Woodlem Park community.

1. In the online environment, students must follow The Woodlem Park Code of Conduct and conduct themselves online as in School.
2. Think before you post. Woodlem Park asks students to use discretion when posting to the internet.
3. Woodlem Park reserves the right to request school-related images or content posted without permission to be removed from the internet.
4. Do not misrepresent yourself by using someone else's identity.
5. Social media venues are public and information can be shared beyond your control. Be conscious of what you post online as you will leave a long-lasting impression on many different audiences.
6. Do not post or link anything (photos, videos, web pages, audio files, forums, groups, fan pages, etc.) to your social networking sites that you wouldn't want friends, peers,

parents, teachers, school admissions officers, or future employers to access. What you present on social networking forums represents you forever.

7. When responding to others, remember to be respectful and avoid comments that may be hurtful. Do not use profane, obscene, or threatening language.

8. Only accept invitations to share information from people you know. Utilize privacy settings to control access to your network, web pages, profile, posts, blogs, wikis, podcasts, digital media, forums, groups, fan pages, etc.

9. Online stalkers and identity thieves are a real threat. Never share personal information, including, but not limited to, Social Security numbers, phone numbers, addresses, birthdates, and pictures with parties you don't know or on unsecure sites.

10. Users should keep their passwords secure and never share passwords with others. If someone tampers with your blog, email, or social networking account without you knowing about it, you could be held accountable.

11. Cyberbullying is considered an act of harassment.

12. 12.Use of Woodlem Park Logos or images on your personal social networking sites is prohibited. If you wish to promote a specific Woodlem Park Activity or event, you may do so only by means of a link to the official Woodlem Park School Facebook account, Twitter account, or YouTube channel.

Parent Social Media Guidelines:

Classroom blogs and other social media are powerful tools that open up communication between students, parents, and teachers. This kind of communication and collaboration can have a huge impact on learning. Woodlem Park School encourages parents to view and participate by adding comments to classroom projects when appropriate.

Parents are required to adhere to the following guidelines:

1. Parents should expect communication from teachers prior to their child's involvement in any project using online social media applications, i.e., Facebook, blogs, wikis, podcasts, etc.
2. Parents will need to sign a release form for students when teachers set up social media activities for classroom use.
3. Parents will not attempt to destroy or harm any information online.
4. Parents will not use classroom social media sites for any illegal activity, including violation of data privacy laws.
5. Parents are highly encouraged to read and/or participate in social media.
6. Parents should not distribute any information that might be deemed personal about Woodlem Park School.
7. Parents should not upload or include any information that does not also meet the Student Guidelines.

Social Media Guidelines for Faculty & Staff:

Personal Responsibility:

Woodlem Park School employees are personally responsible for the content they publish online. Be mindful that what you publish will be public for a long time—protect your privacy.

1. Your online behavior should reflect the same standards of honesty, respect, and consideration that you use face-to-face.
2. When posting to your blog or any social media site be sure you say that the information is representative of your views and opinions and not necessarily the views and opinions of Woodlem Park School.
3. Remember that blogs, wikis and podcasts are an extension of your classroom. What is inappropriate in your classroom should be deemed inappropriate online.

4. The lines between public and private, personal and professional are blurred in the digital world. By virtue of identifying yourself as an X School District employee online, you are now connected to colleagues, students, parents and the school community. You should ensure that content associated with you is consistent with your work at X School District.

5. When contributing online do not post confidential student information.

Disclaimers:

Woodlem Park School employees must include disclaimers within their personal blogs that the views are their own and do not reflect on their employer. For example, "The postings on this site are my own and don't necessarily represent Woodlem Park School District's positions, strategies, opinions, or policies."

This standard disclaimer does not by itself exempt Woodlem Park School employees from a special responsibility when blogging.

Classroom blogs do not require a disclaimer, but teachers are encouraged to moderate content contributed by students.

Profiles and Identity:

Remember your association and responsibility with the Woodlem Park School in online social environments. If you identify yourself as an Woodlem Park School employee, ensure your profile and related content is consistent with how you wish to present yourself with colleagues, parents, and students. How you represent yourself online should be comparable to how you represent yourself in person.

No last names, school names, addresses or phone numbers should appear on Facebook, blogs or wikis. Be cautious how you setup your profile, bio, avatar, etc.

When uploading digital pictures or avatars that represent yourself make sure you select a school appropriate image. Adhere to Employee handout book guidelines as well as your AUP. Also remember not to utilize protected images. Images should be available under Creative Commons or your own.

Personal Use of Social Media such as Facebook, Myspace and Twitter:

Woodlem Park School employees are personally responsible for all comments/information they publish online. Be mindful that what you publish will be public for a long time—protect your privacy.

1. Your online behavior should reflect the same standards of honesty, respect, and consideration that you use face-to-face, and be in accordance with the highest professional Standards.

2. By Posting your comments having online conversations etc. on social media sites you are broadcasting to the world, be aware that even with the strictest privacy settings what you ‘say’ online

should be within the bounds of professional discretion. Comments expressed via social networking pages under the impression of a 'private conversation' may still end up being shared into a more public domain, even with privacy settings on maximum.

3. Comments related to the school should always meet the highest standards of professional discretion. When posting, even on the strictest settings, staff should act on the assumption that all postings are in the public domain.

4. Before posting photographs and videos, permission should be sought from the subject where possible. This is especially the case where photographs of professional colleagues are concerned.

5. Before posting personal photographs, thought should be given as to whether the images reflect on your professionalism.

6. Photographs relating to alcohol or tobacco use may be deemed inappropriate. Remember, your social networking site is an extension of your personality, and by that token an extension of your professional life and your classroom. If it would seem inappropriate to put a certain photograph on the wall - is it really correct to put it online?

7. Microblogging (Twitter etc.) Comments made using such media are not protected by privacy settings as witnessed by the high profile cases like sports stars being disciplined for tweets expressing personal views. Employees should be aware of the public and widespread nature of such media and again refrain from any comment that could be deemed unprofessional.

Social Bookmarking:

1. Be aware that others can view the sites that you bookmark.
2. Be aware of words used to tag or describe the bookmark.
3. Be aware of URL shortening services. Verify the landing site to which they point before submitting a link as a bookmark. It would be best to utilize the original URL if not constrained be the number of characters as in microblogs -- i.e. Twitter
4. Attempt to link directly to a page or resource if possible as you do not control what appears on landing pages in the future.

Woodlem Park School
...For a Sustainable Growth

Electronic Communications Policy

Overview

Electronic communication is necessary to fulfill multiple roles and activities here at Woodlem Park School. Because of the varying types of electronic communication, we will focus on those used primarily here at Woodlem Park School:

- Email
- Videoconferencing
- Digital Signage
- SMS

Email is the official method of communication at Woodlem Park School, both for students and employees. Business is conducted every day via email. Since email has both positive and negative connotations, it is imperative that we recognize that the positive aspects greatly outweigh the negative aspects. However, we must also realize that the negative aspects exist and ensure that this method of communication is used effectively, efficiently, and for its intended purpose.

Videoconferencing tools are used to facilitate conferences and meetings with other institutions, state agencies, or other third-party entities. Since this type of communication conveys not only audio, but video as well, it is particularly important for it to be used for its intended purposes.

Digital signage is used on campus to convey student activities, important academic dates, campus events, and other information to students, employees, and visitors. Since this is also a visual and auditory communication mechanism, it is also important to ensure it is used for its intended purpose as well.

Policy

Regardless of the type of technology being used, electronic communication is meant to serve the needs of the School by sharing information with students, employees, vendors, other state agencies, campus visitors, and other individuals. Because of the unique capabilities of each system it is important to realize that each type of communication method contains unique issues that must be addressed on a case-by- case basis; however, general rules can be set forth to ensure that any communication method is used wisely and according to its intended purpose.

In general, Woodlem Park School's electronic communication mechanisms are to be used to share information with students, employees, vendors, other state agencies, campus visitors, and other individuals.

It is also important to note that the true definition of information sharing at Woodlem Park School is to adequately convey the appropriate knowledge so that the School mission is not hindered but enhanced. This information is always to be distributed under the following assumptions:

Electronic communication from a Woodlem Park School resource…

- …is always understood to represent an official statement from the institution.
- …shall never be used for the creation or distribution of any information that meets the following criteria:
  - Disruptive
  - Offensive
  - Derogatory
  - Specific comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
  - Any information that could be used to sabotage institutional progress
  - Any personally identifiable information
- …shall not be used for personal gain
- …shall not be used extensively for personal use
- …shall not be used to distribute malicious or harmful software or information.

Emergency Notification Policy Overview

Woodlem Park School maintains an emergency notification system that is used to notify students and employees who have opted in to the service via SMS. This system is updated daily to reflect the current student data available so that any notification message will be delivered to the required student and employee list.

Policy

The Woodlem Park School SMS system is to be used, at all times, for emergency purposes or purposes deemed necessary by the Principal or designee only. The notification system is to be used to send messages via text to mobile phones.

At no time shall this system be used for normal messaging, notifications, or otherwise standard contact as this would compromise the importance of these messages and may create an environment where students and employees are able to overlook these types of messages because of the frequency with which they could occur.

With that said, tests of this system shall be conducted once a semester at minimum to ensure the system is functioning properly. Additional tests may be conducted but are not required; however, more than four tests per semester may be too many to retain the importance of such messages when an actual emergency arises requiring the system to be operational.

Only users defined below shall be able to send emergency notification messages via this system:

- School Operations Head / Admin Manager
- IT in charge at school

Password Policy

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of WPS's entire network. As such, all WPS employees (including contractors and vendors with access to WPS systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The policy is applicable to all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that belongs to WPS, resides at any WPS location, has access to the WPS network, or stores any WPS information.

Policy

All passwords will meet the following criteria:

- All system-level passwords (e.g., root, admin, application administration accounts) must be changed at least every 180 days.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 30 days.
- Passwords must NOT be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

Passwords are used for various purposes at WPS. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Very few systems have proper support for one-time tokens (i.e., dynamic passwords that are only used once); therefore, every WPS employee should know how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password or a subset of the password is a word found in a dictionary (English or foreign)

The password is a common usage word such as:

- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software
- The words "WPS", "connors", "state", “School” or any derivation
- Birthdays and other personal information such as addresses and phone numbers
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret) Strong passwords have the following characteristics:
- Contain between 8 and 32 characters
- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Contain at least one number (e.g., 0-9)
- Contain special characters (e.g., ~, !, @, #, $, ^, (,), _, +, =, -, ?, or ,)
- Does not contain a dictionary word in any language, slang, dialect, jargon, etc.
- Does not contain personal information, names of family, etc.
-

Passwords should never be written down or stored online. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Please do not use either of these examples as passwords!

Do not use the same password for WPS accounts as for other non-WPS access. Do not share WPS passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential WPS information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE.
- Don't reveal a password in an email message.
- Don't reveal a password to a supervisor.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.

- Don't share a password with family members.
- Don't reveal a password to co-workers.
- Don’t reveal a password to vendors.
- In short, don’t reveal a password to ANYONE.
- Do not use the "Remember Password" feature of applications .
- Do not write passwords down and store them anywhere in your office.
- Do not store passwords in a file on ANY computer.

Other items to remember:

- If someone demands a password, refer them to this document or have them call the WPS IT Department to determine the validity of their request.
- If an account or password is suspected to have been compromised, report the incident to the WPS IT Department immediately and change all passwords as soon as possible.

Password cracking or guessing may be performed on a periodic or random basis by the WPS IT Department or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Never give your password out to anyone. This may or may not include your supervisor, a friend or relative, a student or part-time worker, or even a co-worker.

Filtering Policy

Online, children can be exposed to material that is inappropriate or even harmful for them. This could be material that is sexually explicit or offensive or violent. It may also be content that is racist and encourages hatred towards particular groups, or material that encourages unsafe behaviour such as eating disorders. Material that is considered inappropriate can vary depending on family and cultural standards or values.

How do children access inappropriate content?

Children and young people may not deliberately seek out inappropriate content. They may be inadvertently exposed to such content through otherwise innocuous activities, such as:

1. unexpected results from online searches
2. clicking on unknown links within websites or emails
3. incorrectly typing a web address or clicking on a pop-up ad
4. Clicking on online game content or prize offers.

In some cases children and young people deliberately access inappropriate material, particularly as they move into adolescence. This can be out of curiosity or to share with peers for the 'shock value' of the content.

What is prohibited online content?

Some content that is considered inappropriate may also be prohibited or illegal in the UAE.

Even though there is a national filter which does a good job of filtering prohibited content it is possible for some of this content to get through. Be sure to check out the UAE laws to understand what kinds of content and behaviour are illegal in the UAE.

In terms of children it is important for parents to try and limit the child's exposure to inappropriate content. A good way to do this is through the use of internet filters.

PC Filters, labels and safe zones enable parents to reduce children's risk of exposure to unsuitable or illegal sites and to set time limits for internet access. When deciding which tools are the most appropriate for your family, it may be useful to consider the level of guidance needed from you and balance this against your children's ages and the range of content they may need to access.

PC filters are computer software programs on your computer which offer a range of different functions to block, screen or monitor inappropriate content. Many filters can also be customised to suit the internet activities of each user. Common features of PC filters include:

1. category blocking which enables the user to select from a range of content categories (for example pornography, violence) and decide which to block and which to allow time controls which allow

users to limit internet access to certain times of the day, including the amount of time a child spends on the internet. This can help ensure children can only use the internet when parents are available to supervise and can restrict late night use which is tempting for some teens

2. logging which enables parents to track and record a history of sites visited by their child service blocking which allows users to block or filter access to certain services, such as peer-to-peer, social networking or online games.
3. Internet filters are no substitute for parental guidance and supervision. No filtering tool can block all unsuitable material. As the internet is vast and constantly changing, lists of blocked sites must be continuously updated for the filter to work effectively. Even then, some undesirable sites may still slip through the filter.

4. Labelling tools attach descriptive tags to websites. Most browsers can read these labels and be programmed to block access to these sites or advise when sites are unsuitable for children.

5. Labelling tools can also complement filtering tools.

6. Websites can be labelled according to how suitable they are for children or to identify the sort of material that they contain, for example, medium-level sexual activity.

7. These tools, together with a web browser, enable users to set levels of access for labelled sites, blocking access to anything above those levels. Some browsers also allow users to restrict access to unlabeled sites.

8. While labelling tools are useful, most websites are still unlabeled.

9. Safe zones are secure networks offering access to a range of sites specially designed for children and therefore with little risk of exposure to inappropriate content. Many safe zones are free of charge but some are subscription based, requiring a special login and password as they are protected from other areas on the internet.

10. The following general tips will help parents manage the risks of inappropriate content for young children, older children and teenagers.

Young children

Young children may come across offensive or illegal online content by accident or with encouragement of others, including older siblings.

The following tips can help you to guide young children in their online activities.

1. At this age children's internet use should be closely monitored. To help with this try to keep the computer in a shared or visible place in the home.
2. Be aware of how your child uses the internet and explore it with them. Bookmark a list of 'Favourites' you are comfortable with your child visiting and teach them how to access this list.
3. Teach your child that not everything on the computer is safe to click on. It can be useful to make a rule for young children to check with an adult before clicking on new or unknown things.
4. Teach your child that there are ways they can deal with material that worries or frightens them—they should not respond if they receive something inappropriate, and should immediately tell a trusted adult if they feel uncomfortable.
5. Teach your child how to close a web page or turn off a monitor and call a trusted adult if they are worried about what they see.
6. If your child is exposed to inappropriate content and appears distressed talk with them about it. If necessary seek professional support.
7. Consider using filters, labels and safe zones to help manage your child's online access.

Older children

Older children may come across offensive online content by accident or they may seek it out with encouragement from peers. The following tips can help older children to manage online content.

1. At this age children's internet use should still be closely monitored. To help with this try to keep the computer in a shared or visible place in the home.
2. Be aware of how your child uses the internet and explore it with them. Explore their favourite sites and help them bookmark a list of 'Favourites'. Discuss the type of content that is and isn't okay online including violent or rude content. This will depend on your family standards.
3. Teach your child that there are ways they can deal with disturbing material—they should not respond if they receive something inappropriate, and they should tell a trusted adult if they feel uncomfortable or worried.
4. Reassure your child that you will not deny them access to the internet if they report feeling uncomfortable or unsafe when online. This is a very real concern for children that may stop them from communicating with you openly.
5. Teach your child how to close web pages that they don't like or to turn off the monitor and call a trusted adult.
6. If your child is exposed to inappropriate content and appears distressed talk with them about it. If necessary seek professional support.
7. Consider using filters, labels and safe zones to help manage your child's online access.

Teenagers

Teenagers may see come across offensive online content by accident or they may seek it out.

The following tips will help teens manage the content they access online.

1. Be mindful that some websites encourage harmful or illegal behaviours such as eating disorders and violent acts. Consider your teen's vulnerability to information and check what they are viewing online.
2. Try to have the computer in a shared or visible place in the home, particularly if your teen is vulnerable; for example, has a mental health issue or behavioural issue.
3. Teach your teens that there are ways they can deal with disturbing material—they should not respond if they receive something inappropriate, and tell a trusted adult if they feel uncomfortable or concerned about themselves or a friend.
4. Reassure teens that you will not deny them access to the internet if they report feeling uncomfortable or unsafe when online. This is a very real concern for teens that may stop them from communicating with you openly.
5. Encourage your teen to look out for friends. If they know a friend is accessing content that seems to be impacting on them negatively encourage them to share their concern with their friend and report it to a trusted adult anonymously if necessary.
6. If your teen is exposed to inappropriate content and appears distressed talk with them about it. If necessary seek professional support.
7. Your child's school may also be able to provide assistance or guidance.
8. Consider using filters, labels and safe zones to help manage your teen's online access.

Woodlem Park School
...For a Sustainable Growth

DATA PROTECTION POLICY

Scope

This document specifies requirements for a Data protection for Woodlem park School; When

- Needs to demonstrate its ability to support & Protect the Data of all enrolled learners. Parents ,Staff and other beneficiaries
- Aims to enhance satisfaction of learners, other beneficiaries and staff through the effective application of data protection policy of Woodlem Park School.
- All requirements of this document are generic and intended to be applicable to all departments of academic and admin sections of The Woodlem Park School, Ajman

DATA PROTECTION PRINCIPLES

Obtain and process Personal Data fairly

Information on students is gathered with the help of parents/guardians and staff. Information is also transferred from their previous schools. In relation to information the school holds on other individuals (members of staff, individuals applying for positions within the School, parents/guardians of students, etc.), the information is generally furnished by the individuals themselves with full and informed consent and compiled during the course of their employment or contact with the School. All such data is treated in accordance with the Data Protection legislation and the terms of this Data Protection Policy. The information will be obtained and processed fairly

Consent

Where consent is the basis for provision of personal data, (e.g. data required to join sports team/After-school activity or any other optional school activity) the consent must be a freely-given, specific, informed and unambiguous indication of the data subject's wishes. Woodlem Park School will require a clear, affirmative action e.g. ticking of

Definitions	
Student	Each learner enrolled at Woodlem Park School Ajman, including those people of determination and those of Special needs.
Parents	Refers to birth parents and other adults who are in a Parenting role.
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.
Staff	Refers to all those working for or on behalf of the school, Full time or part time.
Vendor	Outsource people for required and essential service in Collaboration.
Data	**Academic Context:** All digital resources /modules related with teaching –learning, Assessment and respective record Of assessments made available by the school. **Admin Context:** All valid information about Individual and their Woodlem Park School who is registered as Student, Parent/Guardian, Staff, Vendors & Other Beneficiaries at Woodlem Park School, Ajman
Protection	Securing data of both academic context and Admin context for the mutual growth of the School and Other beneficiaries

Objectives:

- To safeguard the information of all beneficiaries and use it for the mutual benefits.
- To prevent the loss of data and enhance the safety of students during online modes of services/ practices of teaching learning.
- To keep parents updated about wards uses of electronic devices during teaching learning hours.
- To provide flexi environment for modes of operations with vendors of the school.
- To integrate the students wellbeing.

Roles and Responsibilities

The School

- The Woodlem Park School has established a method to deal with the protection and transparency of learners' data and maintain it as documented information. With the following methods
    a) What learner data are collected, and how and where they are processed and stored;
    b) Who has access to the data?
    c) Under which conditions learner data may be shared with third parties;
    d) How long the data are stored for.
- The Woodlem Park School collects and share learners' data with their explicit consent.
- The Woodlem Park School gives learners and other beneficiaries' access to their own data, and the ability to view their own data.
- The Woodlem Park School takes all appropriate measures to ensure that learners' data can only be accessed by authorized persons. Technological protection measures are validated.

Staff

- All teaching staff using shall use only authenticated log in credential to access any information or resources for teaching learning process.
- All admin staff shall use only their authenticated log in credential to access any information or resources for all admin/Office use.
- All teaching staff can add the digital resources in order to cater the needs of learners.
- Staff of Woodlem Park school shall be restricted to use any information related with students/Parents or resources for any individual purposes.

Parents

- All parents shall provide the information about ward based on only official documents released by local/federal Authorities.
- All parents can view the personal information and can request for correction by providing authenticated relevant documents Issued by local/federal Authorities.
- All parents can edit their contact details at point of time , which will be verified by system to authenticate.(Such as OTP Or Activation link)

Students

- All students shall use only authenticated log –in credentials us access their respective accounts.
- All students shall upload the resources such as home work using authenticated log –in credentials.
- All students are advised NOT to Share their log-In ID credentials.

E-Safe School coordinator

- A member of Senior Leadership Team Shall ensure seamless execution e-Safe School Program.
- Shall Coordinate with system administrator to ensure seamless execution e-Safe School Program.
- Shall monitor log records of system.

Data Protection

Data protection is the process of safeguarding important information from corruption, compromise or loss.

The importance of data protection increases as the amount of data created and stored continues to grow at unprecedented rates. There is also little tolerance for downtime that can make it impossible to access important information.

Consequently, a large part of a data protection strategy is ensuring that data can be restored quickly after any corruption or loss. Protecting data from compromise and ensuring data privacy are other key components of data protection.

Storage technologies that can be used to protect data include a disk or tape backup that copies designated information to a disk-based storage array or a tape cartridge device so it can be safely stored. Mirroring can be used to create an exact replica of a website or files so they're available from more than one place. Storage snapshotscan automatically generate a set of pointers to information stored on tape or disk, enabling faster data recovery, while continuous data protection (CDP) backs up all the data in an enterprise whenever a change is made.

Policy on Incident Management

This procedure addresses how incidents should be handled when related to technology. This includes thefts, data corruption, etc.

- Determine scope of incident.
- Fill out the attached Incident Management Form.
- Ensure the supervisor of the employee that reported or caused the incident has been notified.
- Submit form to MSW.
- SLTn will be notified of the incident.
- Resolutions will be drafted given incident scope and individuals involved.

Important Note – Any incident related information should not be circulated in the School communication network for ex- Staff whatsapp group, on group emails, SMS etc. Schools are requested to adhere to the proper escalation process while reporting any incident to the School Management.

Terms and Definitions

Appropriate Measures

Refers to the measures that the Woodlem Park School IT Department is authorized to take to secure Woodlem Park School's computing resources. This may refer to measures concerning Woodlem Park School owned hardware or software, data, employees, students, associates, visitors, etc. The Woodlem Park School IT Department must maintain an appropriate measures option so that Woodlem Park School is protected, concerning both equipment and information.

Approved Electronic File Transmission Methods

Includes supported FTP clients including, but not limited to, FileZilla, SecureFTP, and SmartFTP. This also includes supported Web browsers including, but not limited to, Microsoft Internet Explorer, Mozilla Firefox, Netscape Navigator, and Opera. If you have a business need to use other mailers contact the Woodlem Park School IT Department prior to implementation.

Approved Electronic Mail

Includes all mail systems supported by the Woodlem Park School IT Department. This includes, but is not limited to, Woodlem Park School Webmail, Outlook configured email, and configured email on mobile devices. If you have a business need to use other mailers contact the Woodlem Park School IT Department prior to implementation.

Chain email or letter

An email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck and/or money if the directions are followed.

Information System Resources

Information System Resources include, but are not limited to, all computers, peripherals, data, and programs residing on the Woodlem Park School Campuses, networks, servers, etc. These resources also include all paper information and any information for internal use only and above.

Information Technology Systems

The technology department responsible for managing Woodlem Park School's computing resources.

Configuration of Woodlem Park School-to-Third Party Connections

Connections shall be set up to allow third parties requiring access to the Woodlem Park School campuses, networks, data, etc. These connections will be set up in order to allow minimum access so that third-party entities will only see what they need to see, nothing more. This involves setting up access, applications, and network configurations to allow access to only what is necessary.

Email

The electronic transmission of information through a mail protocol such as SMTP, IMAP, or Exchange. Typical email client include Microsoft Outlook.

Internet

A worldwide, publicly-accessible series of interconnected networks used to transmit packets of data via the Internet Protocol (IP).

Personal Computer

A device used by a single user to access local programs and files, network resources, or the Internet. This can include desktop, laptop, tablet, or portable computers.

Physical Security

Physical security refers to the actual physical security mechanisms in place to prevent unauthorized access to technology resources. This can also mean having actual possession of a computer or by locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room, in a vehicle, on an airplane seat, etc. Make arrangements to lock the device in a secure location such as a hotel safe or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer, cabinet, safe, etc. or simply take it with you.

Public Link

An electronic communications path for which Woodlem Park School does not have control over the entire distance. This connection does not utilize any special connection scheme. A connection from any Woodlem Park School computer to the Internet is an example of a public link.

Secure Internet Links

All network links that originate from a locale or travel over lines that are either under the control of Woodlem Park School or utilize technology to form a secure “pipe” for information to traverse. These types of connections prohibit an unidentified third-party to intercept, monitor, or copy the traffic being sent across this connection by solely utilizing the Woodlem Park School network or utilizing a secure authentication mechanism to connect

Sensitive information

Information is considered sensitive if it can be damaging to Woodlem Park School, IT employees, students, associates, etc. This information can include personnel data, student information, purchasing information, etc.

Unauthorized Disclosure

The intentional or unintentional revealing of restricted information to individuals, either internal or external to Woodlem Park School, who do not have a need to know that information.

User Authentication (Local)

A method by which the user of a system can be verified as a legitimate user on that system only.

User Authentication (Network)

A method by which the user on a network can be verified as a legitimate user independent of the computer or operating system being used.

Virus Warning

Typically, these are emails containing warnings about virus or mal-ware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users. However, the Woodlem Park School IT Department occasionally sends out virus warning should the need arise. In these cases, recipients should heed the warnings provided by the IT Department employees rather than treat the information as potentially misleading.

Disclaimer

The Woodlem Park School IT Department regards this document as a work in progress. Because of this, these policies and procedures undergo regular reviews and modifications. Therefore, it is up to each individual employee or associate to remain current on the updated policies and procedures.

Changes in these policies and procedures after the initial agreement signature date does not allow non-compliance or permit the employee or associate to engage in activities contradictory to the modifications made after the initial agreement signature date.

Forms

Incident Report Form - Student

User Causing/Experiencing Incident:

Name:_____ Class:_____Section:_____Adm No:_____

Incident Date/Time:_____Incident Type:_____Location:_____

Incident Details: _____

Reported By:_____Witnessed By:_____

Reported to :_____Information to Parents: _____

Action Taken: _____

Incident Report Form - Staff

User Causing/Experiencing Incident:

Name:_____ Staff ID:_____

Incident Date/Time:_____Incident Type:_____Location:_____

Incident Details: _____

Reported By:_____Witnessed By:_____

Reported to :_____Information to Management: _____

Action Taken: _____

Woodlem Park School
...For a Sustainable Growth

Internet Safety Tips for Parents

- Talk with your child about Internet safety as soon as he/she begins using the Internet.
- Use age-appropriate filtering, blocking and monitoring software on all Internet-enabled devices used by your child, including laptops, wireless phones and video games.
- Set limits on the amount of time your children are allowed on the internet and get to know the websites your child visits most. Educate yourself about your child's online activities.
- Explain to your child that he/she should never give out personally identifiable information online for example, your child should understand that he/she should not post detailed information about his/her whereabouts.
- Make sure your child knows never to meet someone they met online face-to-face without first talking with you about the situation.
- Explain to your child that they should never share their passwords with anyone including friends.
- Keep a note of your child's mobile phone usage and review text messages etc. from time to time including any sent or received images.
- Educate yourself on the latest threats facing kids online (e.g., cyber bullying, sexting, etc.)

Cyber bullying

Cyber bullying of young people is the result of continual harassment and mistreatment by being made fun of via:

- emails,
- social networks,
- text messages,
- cell phones
- videos
- blogs
- any other form of electronic communication

This repeated and hostile behaviour can be driven by an individual or group.

Cyber Bullying can include the following activities:

a) Posting of slanderous messages on social networking sites

b) Spreading of rumours online

c) Excluding a person from an online group

d) Sending of unsolicited messages via text, instant messaging or email

This kind of victimisation generally occurs any place or any time so that the victim no longer feels safe even in their home. This in turn causes great distress and negative impact on the person's self-esteem and confidence.

If left unchecked, the effects of Cyber bullying can lead to poor grades, emotional spirals, depression, school absences and in some cases, suicide. Unfortunately cyber bullying occurs globally and is currently on the rise!

Impact of cyber bullying

Cyber bullying can happen to anyone, not just vulnerable children and young people. However, cyber bullying is more likely to happen to children who are also bullied offline.

As with offline bullying, cyber bullying can have long lasting consequences and children need support.

Indicators of cyber bullying

Signs that your child may be experiencing cyberbullying include changes in their general behaviour or mood, a decline in physical health, changes in friendship groups, changes in sleep patterns or absences from school or clubs.

If your child does show any of these indicators, and especially if their behaviour is new and out of character for them, talk to them about your concerns and keep a close eye on their online and offline behaviour. Keep them connected to supportive friends and family both online and offline.

Tips to manage cyber bullying

The following practical tips are provided to help parents manage the risks of cyber bullying with young children, older children and teenagers.

Young Children

Cyber bullying is less common between young children with the likelihood of a child being involved in cyberbullying increasing with age.

Cyber bullying can have negative academic, social and psychological outcomes for children, so providing support for children who are involved in cyberbullying is critical.

For young children, general internet safety tips are a good starting point to help them to develop appropriate online etiquette and to learn appropriate responses to bullying behaviours. The following tips are particularly important:

- At this age children's internet use should still be closely monitored. To help with this try to keep the computer in a shared or visible place in the home.
- Keep your child connected online and offline to friends and family that they trust. This helps to protect them from potentially negative outcomes.
- Help your child understand that what they say and do online is important. Encourage your child to use the same manners, communicate with others in the same way and report others who aren't being nice, just as they would in the offline world.
- Advise your child not to respond to any negative messages and to report any negative messages they receive to you or another trusted adult.
- If your child has passwords for their online activities, advise them never to share their password with friends—friendships may be short lived at this age and former friends can misuse passwords to cyber bully.
- If your child has been involved in cyberbullying and seems distressed or shows changes in behaviour or mood it may be advisable to seek professional support,
- Your child's schools may also be able to provide support and guidance.
- If there is a threat to your child's safety the police can help.

Older Children

Cyber bullying occurs most commonly among older children and teens.

Cyber bullying can have negative academic, social and psychological outcomes, so providing support for children and young people who are involved in cyberbullying is critical.

Helping children to manage responses to negative online behaviour and keeping them connected online and offline to friends and family that they trust are important measures to protect them from potentially negative outcomes. The following tips are particularly important:

- At this age your child's internet use should still be closely monitored. To help with this try to keep the computer in a shared or visible place in the home.
- Talk to your child about cyberbullying before it happens. Work out strategies to address cyber bullying that you are both comfortable with, so your child knows what to expect if they do report concerns to you or another trusted adult.

- Reassure your child that you won't block their access to the internet if they report concerns about cyber bullying. Help them to stay connected online and offline to supportive family and friends.
- Help your child to block anyone who sends offensive content. Most social networking services allow users to block and report someone who is behaving badly,
- Advise your child not to respond to any negative messages but to save the messages and details of the senders. You may want to save the messages for your child so that they don't keep reading them and potentially feel worse.
- Encourage children to support their friends and report concerns about friends who may be involved in cyberbullying.
- Help your child to develop the skills they need to interact safely and respectfully online. Guide their online activities and help them learn to communicate appropriately with friends and family.
- Advise your child never to share their password with friends—friendships may be short lived at this age and former friends can misuse passwords to cyber bully.
- If your child has been involved in cyberbullying and seems distressed or shows changes in behaviour or mood it may be advisable to seek professional support
- If there is a threat to your child's safety the police can help. In life threatening and time critical situations.

Teenagers

Cyber bullying occurs most commonly among older children and teens.

Cyber bullying can have negative academic, social and psychological outcomes for children, so providing support for children who are involved in cyberbullying is critical.

For many teens, their online life is an important part of their social identity. Many teens fear that parents might disconnect them from the internet and therefore their supportive friends as a 'solution' to cyber bullying. This prevents some teens from reporting cyber bullying issues. Some teens are also concerned that parents will make cyber bullying issues worse. The following tips are particularly important:

- Talk to your teen about cyber bullying before it happens. Work out strategies to address cyber bullying that you are both comfortable with, so your child knows what to expect if they do report concerns to you or another trusted adult. Reassure them that you will be there to support them and won't disconnect them from their online world.

- Encourage your teen to tell you or another trusted adult if they receive or hear of negative messages, or are excluded by others. Help them stay connected to trusted friends and family both online and offline. This is an important protective measure against the potentially negative outcomes of bullying.
- Advise your teen not to respond to any negative messages but to save the messages and details of the senders. You may want to save the messages for your teen so that they don't keep reading them and potentially feel worse.
- You can help your teen report any concerns to the administrator of the service used, including the mobile phone provider (if SMS is involved), website administrator (if social networking or chat services are involved), or internet service provider.
- Understand your school's policy about cyber bullying—do they have a policy and what is the likely outcome of a complaint about cyber bullying if another student is involved.
- Encourage your teen to support their friends and report concerns about friends who may be involved in cyberbullying.
- Advise your child never to share their password with friends—friendships may be short lived at this age and former friends can misuse passwords to cyber bully.
- If your child has been involved in cyberbullying and seems distressed or shows changes in behaviour or mood it may be advisable to seek professional support.
- If there is a threat to your child's safety the police can help. In life threatening and time critical situations.

Sexting

"Sexting" is generally referred to as a teen or young adult sharing nude photos or lewd text on mobile phones or through online chat. The practice can have legal and physiological consequences as well as long term damage for careers and family later in life.

Sexting is illegal! Don't take or send nude or sexually suggestive photos of yourself or anyone else including sexually suggestive text messages. By doing this or passing on someone else's photos or texts you run the risk of being charged with child pornography. If you keep these messages on your cell phone or computer you could be charged with possession of child pornography. If the messages are sent across state boundaries this becomes a federal offence which generally carries greater penalties in court.

There are also non legal consequences of such behaviour. Emotional damage as well as damage to one's reputation is common. Friendships aren't often lasting so by sharing intimate photos and text with a friend you have no control of what happens to this information if the friendship ends. These

messages can be transmitted and shared with many people or put on the internet as a permanent record. Once this occurs it will be practically impossible to undo the damage to reputation or remove all traces of the personal data.

There are many causes for sexting and this behaviour usually is a result of peer pressure (a form of cyber bullying) or pressure from a boyfriend / girlfriend. Sometimes it can be an impulsive behaviour, flirting or even blackmail. It is always a bad idea to partake in this behaviour.

Parents need to talk with their children about sexting to determine what their child knows about it and also to inform them of the potential consequences of sharing this kind of intimate information. Parents need to express how they feel in a conversational, non-confrontational way. A two-way dialog can go a long way toward helping your kids understand how to minimize legal, social and reputation risks.

Stay alert when using digital media and sharing information. People aren't always who they seem to be and sometimes changes in circumstance can lead to embarrassing and damaging consequences. Critical thinking about what we upload as well as download is the best protection.

Parents

1. If your children have sent any nude pictures of themselves, make sure they stop immediately. Explain that they're at risk of being charged with producing and distributing child pornography. If they've received a nude photo, make sure they haven't sent it to anyone else.
2. Either way, the next most important thing is to have a good talk. Stay calm, be supportive and learn as much as you can about the situation. For example, see if it was impulsive behaviour, a teen "romance" thing, or a form of harassment.
3. Consider talking with other teens and parents involved, based on what you've learned.
4. Some experts advise that you report the photo to your local police, but consider that, while intending to protect your child, you could incriminate another – and possibly your own child. That's why it's usually good to talk to the kids and their parents first. If malice or criminal intent is involved, you may want to consult a lawyer, the police, or other experts on the law in your jurisdiction, but be aware of the possibility that child-pornography charges could be filed against anyone involved.

Teens

1. If a sexting photo arrives on your phone, do not send it to anyone else (that could be considered distribution of child pornography).
2. Talk to a parent or trusted adult. Tell them the full story so they know how to support you. And don't freak out if that adult decides to talk with the parents of others involved – that could be the best way to keep all of you from getting into serious trouble.
3. If the picture is from a friend or someone you know, then someone needs to talk to that friend so he or she knows sexting is against the law. You're actually doing the friend a big favour because of the serious trouble that can happen if the police get involved.
4. If the photos keep coming, you and a parent might have to speak with your friend's parents, school authorities or the police.

How do I deal With It?

1. Think before you post—it could be online forever.
2. Adjust your privacy settings—some things were never meant to be shared.
3. Manage photos or images tagged with your name.
4. Delete any sexting you receive and don't forward anything on.
5. Consider others before you photograph or post.
6. Talk to an adult you trust.

Unwanted sexual contact

Children and young people can communicate with people online who they don't know, or have not met, in real life. While being in contact with new people can be exciting, the anonymity offered by the internet can allow these new contacts to cover their true identities. For example, someone who says they are a 10 year-old girl could actually be a 40 year-old man. This anonymity means that sexual solicitation and online grooming can occur online and are serious risks.

Sexual solicitation is where someone is asked to engage in a sexual conversation or activity or to send a sexually explicit image or information.

Online grooming and procuring of children over the internet is the illegal act of an adult or adults making online contact with a child under the age of sixteen with the intention of facilitating a sexual relationship.

Risk of unwanted sexual contact

Children and young people may increase the risk of unwanted sexual contact in the following ways.

1. Posting provocative photos and messages or using provocative screen names. Many children think they are being mature or funny when using sexually provocative language and images and don't consider that some undesirable people may be attracted to their information.
2. Posting personal information on publicly accessible websites. For example, if children post their full name, address or school/workplace on a social networking website without using the privacy controls, this can be seen by many people that they will not know. Many children aren't aware of the risks in sharing their personal information publicly, so are happy to make all their information visible.
3. Accepting contacts or 'friends' that they don't know on social networking websites or gaming websites. By accepting these people they allow strangers to access their personal information and images. These contacts may be harmless, but they may also be looking to establish a relationship with the child with a sexual purpose in mind.
4. Engaging in social networking or gaming sites designed for teens or adults. This can increase the likelihood of them being contacted by older teens or adults for sexual purposes.

The following practical tips are provided to help parents manage the risks of unwanted sexual contact with young children, older children and teenagers.

Young Children

Some adults befriend children online for sexual purposes. This is called grooming. It is illegal and should be reported to police. In many cases police can prosecute adults seeking children for sexual purposes even if they haven't made face to face contact with a child.

Young children generally won't be using websites that enable direct interaction with others without supervision. The following general tips will help manage who can contact your child online and their responses to inappropriate contact.

1. At this age children's internet use should be closely monitored. To help with this try to keep the computer in a shared or visible place in the home.
2. Be aware of how your child uses the internet and explore it with them. Bookmark a list of 'Favourites' you are comfortable with your child visiting and teach them how to access this list.

3. If your child is at an age where you have begun educating them about strangers and protecting their body it may be useful to expand those lessons to cover online. The appropriate age for this education will vary and is a decision for you and your family.
4. If you are educating your child about their body and keeping it safe it may be useful to make a rule about what is and isn't okay to discuss on the computer and what should be reported to you or a trusted adult. For example, one rule might be 'if anyone asks you about your underwear or 'private parts' when you are on the computer get Mum to check that what they are saying are okay'.
5. Another good rule is for your child to report anything that makes them feel uncomfortable or funny in their tummy.
6. If your child shows changes in behaviour or mood that are concerning including increased or decreased sexualised behaviours, clinginess or withdrawal explore your concerns with them and if necessary seek professional support.

Older Children

Some adults befriend children online for sexual purposes. This is called grooming. It is illegal and should be reported to police. In many cases police can prosecute adults seeking children for sexual purposes even if they haven't made face to face contact with a child.

Older children may become more interested in websites and gaming sites that enable direct interaction with others including teens and adults. The following tips can help to protect your child against unwanted sexual contact.

1. At this age children's internet use should be closely monitored. To help with this try to keep the computer in a shared or visible place in the home.
2. Explore your child's favourite websites. In general it is useful to consider whether you are comfortable with the content of the sites and the potential for contact with others including teens and adults. Is your child socially ready to manage contact from potentially ill meaning strangers?
3. If you agree to your child accessing sites which may allow direct contact with others consider establishing rules about the amount of information they can provide, including not providing their surname, address or school, and not uploading or SMSing images or videos without parental permission.

4. If your child is at an age where you have begun educating them about strangers and protecting their body it may be useful to expand those lessons to cover online contact.
5. The appropriate age for this education will vary and is a decision for you and your family. It may be useful to make a rule about what is and isn't okay to discuss on the computer and what should be reported to you or a trusted adult. For example, one rule might be 'if anyone asks you about your underwear or 'private parts' when you are on the computer get Mum to check that what they are saying is okay'.
7. Some children feel worried about their parent's reaction to things they may have said or done online and this can prevent them reporting genuine concerns. Perpetrators play on this worry and shame to isolate children. To overcome this reassure your child that they can always safely tell you that they feel uncomfortable or worried about what somebody has been saying to them and what they might have been saying and doing in response.
8. If your child shows changes in behaviour or mood that are concerning including increased or decreased sexualised behaviours, clinginess or withdrawal explore your concerns with them and if necessary seek professional support.

Teenagers

Some adults befriend children online for sexual purposes. This is called grooming. It is illegal and should be reported to police. In many cases police can prosecute adults seeking children for sexual purposes even if they haven't made face to face contact with a child.

Many teens use sites that allow them to directly interact with people they don't know offline. There is a risk that the individuals teens connect with may not be who they claim to be, or that they intend to establish a sexual relationship with your teen. The following tips can help guide your teen's behaviour and help keep them safe from unwanted sexual contact.

1. Stays involved in your teen's use of new technologies—keep up to date with the websites they are visiting and explore them with your teen if possible. In general it is useful to consider whether you are comfortable with the content of the sites and the potential for contact with others including adults.
2. Remind your teen to create screen names or IDs that do not indicate gender, age, name or location and are not sexually provocative.

3. Guide your teen to use their privacy settings to restrict their online information to viewing by known friends only.
4. Encourage your teen to keep their online friends online. If they want to meet someone that they haven't met in person, encourage them to ask a parent or another trusted adult to go with them and always meet in public places, preferably during the day.
5. Encourage your teen to be alert to people online who make them feel uncomfortable and to block them. They should report inappropriate contact to the website administrators.
6. Some teens feel worried about their parents' reaction to things they may have said or done online, especially if they think they encouraged online sexual contact. This can prevent them reporting concerns about online contacts. Perpetrators play on this worry and shame to isolate teens from family and friends and encourage teens to trust and confide in them.
7. To overcome this risk reassure your teen that you will always support them and not block heir internet access if they report that they are uncomfortable or worried about what somebody has been saying online.
8. Be alert to changes in your teen's behaviour or mood that are concerning including increased or decreased sexualised behaviours and/or apparent confidence, clinginess or withdrawal, anxiety or sadness and changed interactions with friends. Explore your concerns with them and if necessary seek professional support.

Woodlem Park School
...For a Sustainable Growth

Ecommerce

E-commerce (electronic commerce) or online shopping means conducting business on the Internet and involves selling and buying of goods or services online. Nowadays, many reputable companies are embarking on this mode of conducting business for wider market coverage.

E-security or internet security covers a range of activities to keep electronic information secure. More and more online purchasing and business are conducted every day so it is important for parents to understand how to protect their computer and finances if they are going to partake in e-commerce and purchase things online.

Reputable online shopping websites provide their clients with secure online transactions. Just by sitting in front of a computer, a buyer can confirm his/her purchases and make an online payment. The goods purchased will be shipped and sent directly to the buyer's address.

Unfortunately, online purchases can sometimes cause you hassle in the form of delayed delivery of goods, the quality of goods does not match the description on the website or the goods never arrive!

Basic Tips for Parents

- Poor e-security or internet security can result in the corruption of files and can enable criminals and others to access personal and financial information. E-security measures provide protection from unwanted intentional and unintentional intrusion into computers, file corruption and data loss. Ensure you have the latest computer security programs such as virus checkers, up to date web browsers and malware detection in place before partaking in e-commerce.

- E-security or internet security covers a range of activities to keep electronic information secure. It is advised that parents familiarise themselves with best practice to ensure they are not victims of an e-security breach.

- Poor e-security or internet security can result in the corruption of files and can enable criminals and others to access personal and financial information.

What to do before making an online transaction?

Online websites provide specific information that is important to pay attention to before conducting online transactions. This includes:

1. The seller's name, address and telephone number
2. The seller's e-mail address (if available)
3. A description of the goods or services
4. The total price and a detailed statement of the terms of payment
5. The date the goods or services will be supplied
6. The currency under which amounts owing are payable
7. An explanation of how the goods will be shipped to you
8. The seller's return or exchange policy, if any
9. You must be given a copy of the contract
10. The website must have a secured protocol
11. Beware of Wi-Fi hotspots. Unknown hotspots are not secure and allow hackers to capture any and all data that's flowing to and from the hotspot, enabling them to steal personal and confidential information (logins, passwords, email messages, attached documents) stored on your mobile device.
12. Look for websites that provide secure payment (known as an encryption) – a padlock icon will be shown on the screen while you are filling in the payment details

13. Beware of scams and unsolicited offers. The advertised website could be malicious, and download malware to your computer. Or it could be a scam, meaning you would never receive what you ordered!

14. Do not trust the search engine results. Search Engine Optimization attacks are a way for cybercriminals to game a search engine's ranking algorithm in order to push websites to the top of keyword search lists.

15. Beware of emails saying "Hey, check out the holiday sale going on here!" or "This place has a 50 per cent off Eid sale!" The sender's computer could be unknowingly infected by malware programmed to go through email address books and send malicious links to everyone in them.

16. Protect your privacy. Do not simply disclose your personal details.

17. Double check whether the company has a privacy statement that tells you what they will do with your personal information.
18. Make sure you know the trader's full details. Those details can be used as backup information if you need to lodge a fraud report. If the seller does not disclose the necessary information, you are recommended to find another seller.

What can you do to protect yourself?

- Check on the product through phone or e-mail.
- Pay by credit card and keep track of all transactions.
- If you are paying online, make sure the website is secure. You need to look for the company security seal or a security statement.

Online Banking

Online banking is defined as an online banking system that offers just about every traditional service available through a local branch. It enables the clients of the bank to conduct banking transactions much faster via the Internet. Despite the advantages of online banking, customers also face risks such as identity theft and credit card fraud. The following tips can help ensure a secure online transaction.

1. Keep your passwords, Personal Identification Number (PIN) and card numbers confidential. Do not share your password or PIN with anyone. Change your password regularly and use different passwords for different websites. Make it difficult for others to guess your password by using a combination of letters and numbers.

2. Look for the lock icon before entering personal information on a website, look for the “lock” icon in your browser. A closed lock or padlock indicates that the website is secure. Another feature of a secure website is the when the URL starts with ‘https: //’.

3. Use a firewall: Install the latest firewall program on your computer to track intrusions.

4. Install computer security updates. Most computers operating systems enable users to update their computer’s security system to protect the data from spyware, viruses and other threats.

Woodlem Park School
...For a Sustainable Growth

Inappropriate content

Online, children can be exposed to material that is inappropriate or even harmful for them. This could be material that is sexually explicit or offensive or violent. It may also be content that is racist and encourages hatred towards particular groups, or material that encourages unsafe behaviour such as eating disorders. Material that is considered inappropriate can vary depending on family and cultural standards or values.

How do children access inappropriate content?

Children and young people may not deliberately seek out inappropriate content. They may be inadvertently exposed to such content through otherwise innocuous activities, such as:

- unexpected results from online searches
- clicking on unknown links within websites or emails
- incorrectly typing a web address or clicking on a pop-up ad
- Clicking on online game content or prize offers.

In some cases children and young people deliberately access inappropriate material, particularly as they move into adolescence. This can be out of curiosity or to share with peers for the 'shock value' of the content.

What is prohibited online content?

Some content that is considered inappropriate may also be prohibited or illegal in the UAE. Even though there is a national filter which does a good job of filtering prohibited content it is possible for some of this content to get through. Be sure to check out the UAE laws to understand what kinds of content and behaviour are illegal in the UAE.

In terms of children it is important for parents to try and limit the child's exposure to inappropriate content. A good way to do this is through the use of internet filters.

PC Filters, labels and safe zones enable parents to reduce children's risk of exposure to unsuitable or illegal sites and to set time limits for internet access. When deciding which tools are the most

appropriate for your family, it may be useful to consider the level of guidance needed from you and balance this against your children's ages and the range of content they may need to access.

PC filters are computer software programs on your computer which offer a range of different functions to block, screen or monitor inappropriate content. Many filters can also be customised to suit the internet activities of each user. Common features of PC filters include:

1. category blocking which enables the user to select from a range of content categories (for example pornography, violence) and decide which to block and which to allow time controls which allow users to limit internet access to certain times of the day, including the amount of time a child spends on the internet. This can help ensure children can only use the internet when parents are available to supervise and can restrict late night use which is tempting for some teens

2. logging which enables parents to track and record a history of sites visited by their child service blocking which allows users to block or filter access to certain services, such as peer-to-peer, social networking or online games.

3. Internet filters are no substitute for parental guidance and supervision. No filtering tool can block all unsuitable material. As the internet is vast and constantly changing, lists of blocked sites must be continuously updated for the filter to work effectively. Even then, some undesirable sites may still slip through the filter.

4. Labelling tools attach descriptive tags to websites. Most browsers can read these labels and be programmed to block access to these sites or advise when sites are unsuitable for children.

5. Labelling tools can also complement filtering tools.

6. Websites can be labelled according to how suitable they are for children or to identify the sort of material that they contain, for example, medium-level sexual activity.

7. These tools, together with a web browser, enable users to set levels of access for labelled sites, blocking access to anything above those levels. Some browsers also allow users to restrict access to unlabelled sites.

8. While labelling tools are useful, most websites are still unlabelled.

9. Safe zones are secure networks offering access to a range of sites specially designed for children and therefore with little risk of exposure to inappropriate content. Many safe zones are free of charge but some are subscription based, requiring a special login and password as they are protected from other areas on the internet.

10. The following general tips will help parents manage the risks of inappropriate content for young children, older children and teenagers.

Young children

Young children may come across offensive or illegal online content by accident or with encouragement of others, including older siblings.

The following tips can help you to guide young children in their online activities.

1. At this age children's internet use should be closely monitored. To help with this try to keep the computer in a shared or visible place in the home.
2. Be aware of how your child uses the internet and explore it with them. Bookmark a list of 'Favourites' you are comfortable with your child visiting and teach them how to access this list.
3. Teach your child that not everything on the computer is safe to click on. It can be useful to make a rule for young children to check with an adult before clicking on new or unknown things.
4. Teach your child that there are ways they can deal with material that worries or frightens them—they should not respond if they receive something inappropriate, and should immediately tell a trusted adult if they feel uncomfortable.
5. Teach your child how to close a web page or turn off a monitor and call a trusted adult if they are worried about what they see.
6. If your child is exposed to inappropriate content and appears distressed talk with them about it. If necessary seek professional support.
7. Consider using filters, labels and safe zones to help manage your child's online access.

Older children

Older children may come across offensive online content by accident or they may seek it out with encouragement from peers. The following tips can help older children to manage online content.

1. At this age children's internet use should still be closely monitored. To help with this try to keep the computer in a shared or visible place in the home.

2. Be aware of how your child uses the internet and explore it with them. Explore their favourite sites and help them bookmark a list of 'Favourites'. Discuss the type of content that is and isn't okay online including violent or rude content. This will depend on your family standards.

3. Teach your child that there are ways they can deal with disturbing material—they should not respond if they receive something inappropriate, and they should tell a trusted adult if they feel uncomfortable or worried.

4. Reassure your child that you will not deny them access to the internet if they report feeling uncomfortable or unsafe when online. This is a very real concern for children that may stop them from communicating with you openly.

5. Teach your child how to close web pages that they don't like or to turn off the monitor and call a trusted adult.

6. If your child is exposed to inappropriate content and appears distressed talk with them about it. If necessary seek professional support.

7. Consider using filters, labels and safe zones to help manage your child's online access.

Teenagers

Teenagers may see come across offensive online content by accident or they may seek it out.

The following tips will help teens manage the content they access online.

1. Be mindful that some websites encourage harmful or illegal behaviours such as eating disorders and violent acts. Consider your teen's vulnerability to information and check what they are viewing online.

2. Try to have the computer in a shared or visible place in the home, particularly if your teen is vulnerable; for example, has a mental health issue or behavioural issue.

3. Teach your teens that there are ways they can deal with disturbing material—they should not respond if they receive something inappropriate, and tell a trusted adult if they feel uncomfortable or concerned about themselves or a friend.

4. Reassure teens that you will not deny them access to the internet if they report feeling uncomfortable or unsafe when online. This is a very real concern for teens that may stop them from communicating with you openly.

5. Encourage your teen to look out for friends. If they know a friend is accessing content that seems to be impacting on them negatively encourage them to share their concern with their friend and report it to a trusted adult anonymously if necessary.

6. If your teen is exposed to inappropriate content and appears distressed talk with them about it. If necessary seek professional support.

7. Your child's school may also be able to provide assistance or guidance.

8. Consider using filters, labels and safe zones to help manage your teen's online access.

Protecting Personal Information

Personal information is any information that identifies an individual. Personal information includes full name, address, date of birth, phone numbers, email addresses, usernames and passwords, bank details, student identity card details or passport details.

Online, personal information is used by many businesses to verify a user's identity. While personal information can be safely disclosed to many legitimate businesses, if not managed carefully, it can be accessed and misused by criminals. It can also be used by marketers who may send spam through email or SMS.

Disclosing personal information online can also impact on a user's 'digital reputation'. A Digital reputation is the opinion that others hold about people based on what they do and say online. The following general tips will help parents protect personal information for your child online.

Young Children

The following guidelines are a useful starting point to teach young children to interact safely and responsibly online.

1. At this age children's internet use should still be closely monitored. To help with this try to keep the computer in a shared or visible place in the home.

2. Be aware of how your child uses the internet and explore it with them. Explore their favourite sites and help them bookmark a list of 'Favourites'. Check whether personal information is required to sign up any of their favourite websites or games and help your child sign up and use privacy settings safely if you feel it is appropriate.

3. Talk to your child about personal information and why it is special. This sort of information can be used to identify or locate where they live, go to school or activities in which they are involved.

4. Set rules to make sure your child knows what information they can share or post online and which websites they can visit. Telling a trusted adult before posting any personal information online, including for competition entry is a useful rule.

5. Consider creating a family 'fun' email account that can be used for competition entries and other activities. This account will be separate to all other personal accounts so it can easily be deleted if it is misused.

Older Children

The following general guidelines are a useful starting point to teach older children to use their personal information safely and responsibly online.

1. At this age children's internet use should still be closely monitored. To help with this try to keep the computer in a shared or visible place in the home.

2. Be aware of how your child uses the internet and explore it with them. Explore their favourite sites and help them bookmark a list of 'Favourites'. Check whether personal information is required to sign up any of their favourite websites or games and help your child sign up and use privacy settings safely if you feel it is appropriate.

3. Talk to your child about personal information and why it is special. This sort of information is information that can be used to identify or locate them and where they live, go to school or join in activities.

4. Set rules—make sure your child knows what information they can share or post online and which websites they can visit. Telling a trusted adult before posting any personal information online, including for competition entry is a useful rule.

5. Remind your child that not everybody online is who they say they are and encourage them to be cautious when sharing information.

6. Help your child to create screen names or IDs that do not communicate their gender, age, name or location.

7. Consider creating a family 'fun' email account that can be used for competition entries and other activities. This account will be separate to all other personal accounts so it can easily be deleted if it is misused.

Teenagers

The following tips can help teens manage their personal information safely and responsibly.

1. Remind your teen that not everyone is who they claim to be. Although they may enjoy having many online friends, adding people that they don't know on 'friends lists' allows those people to learn all about them. This information could be used for scams, to steal their identity or worse.

2. Talk to your teen about managing personal information on social networking sites.

3. Encourage them not to put any personal information on their profiles. This includes their phone number, personal email address, home or school addresses, or the name of their school.

4. Encourage your teen to be careful when they post photos that they are not accidentally providing clues to personal information such as their school uniform.
5. Encourage your teen to set up a separate email account for use when signing up to games or websites. This account will be separate to all other personal accounts so they can disable it if it's misused. It should not include their names or other identifiers in the address.

6. They might also like to set up a separate social networking account if they want to promote themselves or an interest and engage with likeminded people that they don't know offline. They should ensure the site does not contain their personal information.

7. Encourage your teen to read user agreements and privacy policies to determine how their personal information may be used when signing up to services as many organizations use information for their own marketing and some sell it to other marketing firms.

8. Remind your teen that they should only disclose financial information on websites that they trust and that have secure payment facilities identified by a web address beginning with https:// and a 'locked' padlock symbol in the bottom of the screen, which indicates that data is being encrypted.

9. Remind your teen that banking institutions will never email individuals asking for their user name or password. If they receive an email from an organisation claiming to represent a banking institution they should report the email to the bank.

Woodlem Park School
...For a Sustainable Growth

Understanding internet security risks

Poor e-security can result in the corruption of files and data, loss of privacy and can enable criminals and others to access personal and financial information. E-security measures provide protection from unwanted intentional and unintentional intrusion into computers, file corruption and data loss.

Viruses, worms and trojans

A virus is a piece of malicious computer code transmitted by email, through infected downloads including new software, images, music files, infected computer devices such as a USB or when surfing the web. Viruses can damage computers, steal information and spread themselves to other computers.

A Trojan is a program which can damage a computer, steal private data, give other people access to the computer or spread a virus.

A worm is a self-replicating program that can spread without user intervention. Worms are designed to further infect computers with other types of malicious software, such as programs that send spam. A worm can spread by sending itself to all the contacts in an email program's address book, or via a security flaw in a program or in the computer's operating system.

What happens if my computer is infected?

The most common symptoms that a computer has been infected by a virus include:

1. Files and data have been deleted or file names are changed,
2. The computer takes longer to load programs or applications or web pages ,
3. The computer takes longer to boot, continually restarts or does not start at all,

4. Items and images on the screen are distorted and unusual images and text appear,

5. The hard disk may be inaccessible or appear to be working harder than normal,

6. Excessive network activity (lights blinking excessively on modem),

7. The web browser opens on a different homepage,

8. Frequent system or program crashes.

This is not an exhaustive list and these symptoms may occur for reasons other than a virus infection. Seek advice from a computer professional if you suspect your computer may have become infected by a virus.

Spyware and Adware

Spyware is a computer program that is remotely installed on computers, usually without permission from the owner, with the purpose of collecting information and sending it back to another source. Spyware can be a minor annoyance or a serious threat to computer security. At its most aggressive, spyware can be used to steal personal information, banking details and passwords.

Adware is a form of spyware that records a user's web-surfing habits and displays advertisements targeted to their interests. Adware is sometimes offered in exchange for 'free' services, such as music downloads.

Scams, spam and phishing

Scams are ways of obtaining information or money through false means, scams target people of all backgrounds and succeed for two reasons. Firstly, a scam looks like the real thing and secondly, it appears to meet a need, offering quick cash, asking for a response to a compassionate issue, or making people feel special, for example. 'Congratulations you are one of the lucky few chosen… Spam is an unsolicited commercial electronic message. This includes email, instant messaging, SMS and MMS received without consent, usually advertising a product or service. Spam can waste time and lead to viruses. Although the most common place to find spam is in an email, it can also appear in online forums, instant messaging chats, newsgroups and blogs.

Phishing is the use of email or SMS to encourage individuals to reveal financial details like credit card numbers, account names and passwords or other personal information.

Phishing messages can look like genuine messages from a real bank, telecommunications provider, online retailer or credit card company. Often the message will contain an urgent 'call to action', such as claims that the bank account will be closed or compromised if action is not taken. Phishing is usually sent by email from falsified email addresses, but is increasingly being sent to mobile telephones and VoIP telephone services.

Tips for managing scams, spam and phishing

1. Avoid giving out your email address or mobile phone number publicly and check that children aren't giving details out.

2. Check the terms and conditions of anything you and your children sign up for— for example, are you consenting to receive commercial messages?

3. Warn children and young people to be wary about accepting unknown friends or causes on social networking sites—unknown contacts or causes have been linked to identity theft scams.

4. Do not respond to unknown SMSs asking you or your children to make contact and provide cash or financial information. If a phone or email contact seems unusual especially if money is involved hang up or not reply.

5. If concerned that you or your child may have been the target of a scam, contact your local consumer affairs agency.

6. Remember that banking institutions will never contact customers by email seeking specific account details. Contact your bank directly using verified contact details if you have any concerns about a contact from a source claiming to be your bank.

7. Only disclose financial information on websites that you trust and that have secure payment facilities identified by a web address beginning with https:// and a 'locked' padlock symbol in the bottom of the screen, which indicates that data is being encrypted.

8. If you receive an email that seems suspicious, for example, you don't recognise the sender or the subject line looks dubious delete it and don't click on any links within it.

9. If you receive a message from a legitimate business, for example a financial institution or shop, but do not want to receive messages from that organisation, you can unsubscribe through an email link or SMS 'STOP'.

10. Install and update anti-virus and other e-security software to restrict unauthorised access to data on the home computer and protect that data from corruption. Ensure that security features including a firewall are turned on, set to automatic scan and updated regularly to protect against the latest risks.

Pop-ups

Pop-ups are small windows that appear in front of an internet browser. They are frequently used to display advertising, including advertising for unwanted content such as pornography. Pop-ups are also used by many websites to enable users to enter required information legitimately.

Pop-ups used for advertising can annoy users, as they can appear without notice or warning. They can also open websites which are difficult to close, or link users to other, unwanted website content. There are a number of ways to manage pop-ups using settings on search engines or internet browsers. For example, the Google toolbar provides a free pop-up blocker that enables users to configure those websites where they want to allow pop-ups to appear, and to block pop-ups on websites where they aren't required.

A number of popular browsers allow users to change settings to block pop-ups. Check the 'Help' options on these browsers for information.

There are some legitimate websites that invite users to switch off pop-up blocking software temporarily because a pop-up from that site will help the user to enter information required by the site. If it's a reputable website, you can temporarily turn off pop-up blocking.

Woodlem Park School
...For a Sustainable Growth

Social Media

Social networking describes a variety of online services like Facebook, YouTube, MySpace, Twitter, online games such as World of Warcraft and Moshi Monsters and virtual worlds such as Club Penguin. These services let people communicate with others online. This can enable young people to stay in touch with friends and family and join in fun fantasy worlds and games. However, children may forget who they are communicating with online and disclose too much about themselves. They may also behave in ways that they wouldn't offline.

"Social networking services" refers here to a wide-range of rapidly developing services tools and practices. Social networking services can be broadly defined as Internet- or mobile-device-based social spaces designed to facilitate communication, collaboration and content sharing across networks of contacts.

Social networking services allow users to manage, build and represent their social networks online. Services usually (but not always) include other individuals; they might also include the profiles of events, companies, even political parties. They may let you add anyone in the network as your friend or contact, or they might ask both parties to agree to all connections.

Social networking services typically support the public display of networks, although they may offer privacy restrictions or facilitate closed communities. Permissions are a very important feature of most social networking services. They allow members and groups to control who can access their profiles, information, connections and spaces, as well as determining degrees of access. The level of granularity and control varies from service to service. Typically settings allow you to keep your information private (i.e. be seen by only those to whom you give permission) or restrict the visibility of your information to:

1. Signed-in service members only,

2. People on your contacts list,

3. Particular groups of service users,

4. Make your information public so that even people who are not members or are not signed in as members of the service can see it.

Through these combinations of privacy settings, users can manage a range of different relationships online, as well as manage their online presence – how they appear to friends, acquaintances or the general public.

Managing relationships online and managing your online presence are key to having fun with and using social networks safely. However, the speed of the development of social networking services may mean that young people are more likely to have developed personal strategies or learnt from peers than from formal instruction and support from adults.
Social networking sites vary in the types of tools and functionality they provide, by definition social networking sites as having three common elements:

1. A member profile (in their definition this is always a web page),

2. The ability to add other members to a contact list,

3. Supported interaction between members of contact lists (interaction varies greatly, and there will typically be some degree of interaction facilitated between people who are not on each other's contacts lists).

Social networking sites are often perceived by their users as closed environments, where members talk to other members. This impression of social networking services as providing a private space is likely to account for behaviour, language and postings that do not translate well outside their intended closed context. While it is important that children and young people understand the public nature of much of their activity within social networking services (and can use permissions and privacy controls to manage personal information and communications), we also need to ensure that online activity is understood holistically – i.e. as the sum of activity of all the online sites and networks that an individual belongs to.

Issues and complaints when using a social networking site

Concerns about social networking sites can be reported to the website administrator in first instance. Look for the contact address on the site. Many sites have 'report' buttons or a contact centre to help address issues around safety, offensive content, hacking and scams.

Users can also seek independent legal advice about the options they may have for dealing with the material concerned.

The following general tips will help parents manage the risks of social networking for young children, older children and teenagers.

Young children

Generally young children will have little direct involvement in social networking as they will not meet the recommended age guidelines. There are some social networking sites targeted at children that claim to moderate communication to provide greater protection for children. Your child may ask to use one of these websites at some stage, and the following tips may be useful.

1. If your child is using social networking services, including gaming sites and virtual worlds that allow them to communicate directly with other people check the age guidelines and privacy policies of the sites. Check how moderation occurs—do they administrators check all messages before they are published? Are you comfortable that your child is safe interacting on the website?

2. Set rules—make sure your child knows what information they can share or post online and which websites they can visit. Ask them to tell you before they post any personal information online, including their full name, mum or dad's name, their address or school.
3. Help your child to create screen names or IDs that do not communicate their gender, age, name or location.

4. Establish rules around the types of content or information they should report to an adult. For example, one rule may be 'tell Mum or Dad if somebody asks you where you go to school or where you live' and 'tell mum and dad if anybody talks about rude things'.

5. Advise your child to check with you before clicking on links sent by others on social networking websites. These may lead to adult content.

6. Help your child understand that what they say and do online is important. Encourage your child to use the same manners, communicate with others in the same way and report others who aren't being nice, just as they would in the offline world.

7. Advise your child not to respond to any negative messages and to report any negative messages they receive to you or another trusted adult.

Older children

1. If your child is using social networking services check the website age guidelines and terms and conditions. In general it is useful to consider whether you are comfortable with the content and the potential for contact with others including teens and adults. Is your child socially ready to manage contact from potentially ill meaning strangers?

2. Help your child set up their profile to make sure that they don't put too much personal information online. Help your child to create screen names or IDs that do not communicate their gender, age, name or location and are not sexually provocative.

3. Set rules—make sure your child knows what information they can share or post online. Ask them to tell you before joining new websites and before they post any personal information online, including their full name, address or school.

4. Advise your child not to respond to any negative messages and to report any negative messages they receive to you or another trusted adult.

5. Establish rules around the type of contact they should report to an adult. For example, one rule may be 'tell Mum if somebody asks you about your underwear or private parts'.

6. Reassure your child that you will not deny them access to the internet if they report feeling uncomfortable or unsafe when online. This is a very real concern for children that may stop them from communicating with you openly.

7. Advise your child to check with you before clicking on links sent by others on social networking websites. These may lead to adult content.

8. Remind your child to communicate appropriately with others online, and to report any bullying of themselves or others to you or another trusted adult.

9. Talk to your child about the use of location based services. These services enable social networking users to report their physical location to other users by 'checking in'. Some services let people report their friends' locations and have location based functions turned on by default. Your child can review their settings and block this function or limit who sees their location based information. Remind your child that allowing strangers to see where they are, or where their mates are, is a risky behaviour.

10. You may also like to contact your mobile phone company for assistance with blocking internet, Bluetooth and GPS functionality on their child's mobile phone to limit their ability to notify others of their whereabouts.

11. Consider using filters, labels and safe zones to help manage your child's online access.

Teenagers

1. Talk to your teen about managing personal information on social networking websites. Encourage them not to put key personal information on their profiles. This includes their phone number, home or school addresses, information about workplaces or clubs.

2. Remind your teen not to post photos of themselves or others that they would not want strangers to see, or that may have a negative impact on how others view them.

3. Ensure your teen understands the privacy features—in particular how to set their profile to private and limit access to their information. Encourage teens to screen online 'friends'.

4. Remind your teen that not everyone is who they claim to be. Although they may enjoy having many online friends, adding people that they don't know on 'friends lists' allows those people to learn all about them. This information could be used for scams or cyber stalking.

5. Talk to your teen about the use of location based services. Services such as Foursquare and Facebook enable social networking users to report their physical location to other users by 'checking in'. Some services let people report their friends' locations and have location based functions turned on by default. Your teen can review their settings and block this function or limit who sees their location based information. Remind your teen that allowing strangers to see where they are, or where their mates are, is a risky behaviour.

6. You may also like to contact your mobile phone company for assistance with blocking internet, Bluetooth and GPS functionality on their child's mobile phone to limit their ability to notify others of their whereabouts.

7. Encourage your teen to keep their online friends online. If they do want to meet someone that they haven't met so far in person, they should ask a parent or another trusted adult to go with them and always meet in a public place, preferably during the day.

8. Remind your teen not to respond if someone sends them negative messages or asks them to do something that makes them feel uncomfortable. They should tell a trusted adult and save the messages.

9. Encourage your teen to set up a separate social networking account if they want to promote themselves or an interest and engage with like-minded people that they don't know offline. They should ensure the site does not contain their personal information.

The Policy Disclaimer

The policies included on this manual are not legal documents. Every attempt has been made to accurately represent the policies and benefits programs. The policies and procedures described here are based on plan documents and ministerial policies that governs the operations of the policies. The Woodlem Park School may add, modify, or remove portions of these Policies when it is considered as appropriate to do so, and any such changes will be effective upon giving notice of the revised policy. We periodically review policies and procedures in part or as a whole, to ensure that they continue to reflect current thinking in the field of safeguarding and are consistent with trends and legislative requirements.

Policy Agreement

We, the Woodlem Park School, Ajman accept 'The Whole school policy; E- safety' to serve the purpose of educating the safety and wellbeing of children and young people when adults, young people or children are using the internet, social media or mobile devices, to provide staff and volunteers with the overarching principles that guide our approach to online safety and to ensure that, as an organization, we are an E- safe school operating in line with our values and within the law in terms of how we use online devices during the remote learning mode of education. This policy and procedures applies to all the beneficiaries of the Woodlem Park School, Ajman with effective from 15th September 2020.

Signature of the Principal: ***Signature of the Managing Director***

Policy Consent

I ……. Staff/ student/ parent hereby acknowledge that I have read the 'The Whole school policy; E- safety', familiarized with its contents, and adhering to all of the policies, procedures, and protocols of the Woodlem Park School, to ensure the online safety and security of the whole school community.

Signature: