LEADERS PRIVATE SCHOOL, SHARJAH

E-Safety Policy

It is the responsibility of all members of the school to ensure that they are following the current version.

Document Details

Information Sharing Category	Public
Updated on	February 2024
Next Review Date	March 2025

Table of Contents

Introduction

This policy should be read in conjunction with the National Child Protection Policy in Educational Institutions in United Arab Emirates, *IT Policy, Privacy Policy, E-Learning Policy, Behaviour Policy, Behaviour Management Policy-MOE, Behaviour Policy for Distance Learning-MOE, the Child Protection Policy , the Anti-bullying Policy Cyber-Bullying Policy , Staff AUP and Student AUP*

The school fully recognizes its duty to protect all of its members and to provide a safe, healthy online environment for everyone.

The aim of the E-Safety policy is to ensure that all students and Staff are aware of the risks and hazards of internet usage and use it sensibly and safely for the purpose of information sharing and improved learning. All students and Staff should be free of any fear of cyber bullying by anyone known or unknown, should be able to recognize cyber bullying and be fully equipped to be able to deal with it effectively as well as are fully competent in surfing internet safely.

We are committed to helping all members of the school community to benefit from information and communication technology, while understanding its risks, and to equip children with the knowledge and skills to be able to use it safely and responsibly.

The school recognizes that any bullying incident should be treated as a child protection concern when there is reasonable cause to believe that a child is suffering or likely to suffer significant

Purpose

This E-Safety policy enables our school to create a safe e-learning environment that:

- Protects children from harm and cyber bullying
- Safeguards staff in their contact with students and their own use of the internet
- Provides clear expectations for all on acceptable use of the internet.

Scope of the policy

This policy includes:

- E-Safety Roles & Responsibilities
- Cyber Bullying
- Social Media Access
- Rules for publishing material online
- Data Protection
- Communications
- Technology Platforms
- Password Policy
- Network and Internet Access
- Use of Mobile Device
- Reporting an Incidents
- Disciplinary Procedure

E-Safety Roles & Responsibilities

Principal & SLT

- The school's Principal is responsible for :
  - The approval of the E-Safety Policy and for reviewing the effectiveness of the policy.
  - Regular meetings with the E-Safety Officer
  - Regular monitoring of E-Safety incident logs
- The Principal and Senior Leadership Team should :
  - Ensure that the safety (including E-Safety) of members of the school community
  - be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a student/ member of staff
  - Ensure that the E-Safety Officer and other relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
  - Provide curriculum about appropriate etiquette for online behavior, including awareness about interactions and communication with others on social networking websites and in chat rooms
  - Organize workshops on raising awareness of cyber bullying & E-Safety.
  - Ensure safety and security of students when using internet and electronic communications
  - Provide students, staff and parents with guidelines and instructions for student safety while using the Internet

E-Safety Officer

- Act as a named point of contact on online safety issues.
- Ensure policies and procedures that incorporate online safety concerns are in place.
- Record online safety incidents and actions taken, in accordance with the school's child protection policy.
- Ensure the whole school community is aware of what is safe online behaviour and understand the sanctions for misuse.
- Work with the leadership team and technical support staff, to ensure that appropriate filtering and monitoring is in place.
- Implement regular online safety training for all members of staff.
- Work with staff to ensure that online safety education is embedded in the curriculum.
- Ensure that online safety is promoted to parents and the wider community through a variety of channels.
- Ensure that their own knowledge and skill are refreshed at regular intervals.
- Evaluate the delivery and impact of the online safety policy and practice.
- Review any reported online safety incidents to inform and improve future areas of teaching, training and policy development.
- Feedback online safety issues to the management/leadership team and other agencies, where appropriate.

Online Safety Group:

- The schools Online Safety Group comprises of the School's Principal, SLTs, E-Safety Officer, Teachers, Doctor, Social Worker and Members from the student Council.
- Online safety groups should meet as regularly as deemed necessary by the setting.
- Online safety groups can support many of the associated tasks, on behalf of the online safety lead, such as:
  - Producing and reviewing policies
  - Mapping, planning and reviewing the online safety curriculum
  - Producing, reviewing and monitoring the school filtering policy
  - Consulting with stakeholders
  - Raising awareness throughout the community

- Auditing online safety practice and policy compliance
- Reporting regularly to the governing body to help inform them of existing practice and localized concerns
- To use the wide and varied knowledge of others with different skills.
- To monitor the impact of online safety education and to identify and fill any gaps.
- To raise and manage new initiatives including annual initiatives such as anti-bullying week and Safer Internet Day.
- To monitor incidents and establish the best way of dealing with them.
- To engage the community - working together to benefit all.

Counsellor:

- Acting as a key member of the school's internet safety team, liaising with the E- safety officer on specific incidents of misuse, and providing follow-up counselling and support to both victims and perpetrators as appropriate
- Taking a proactive role in the internet safety education of students
- Developing systems and procedures for supporting and/or referring on students referred to them as a result of breaches of internet safety within schools
- Developing systems and procedures for students who self-refer, and those students identified as suspected 'victims' by teaching staff
- Seeking professional development on the safety issues relating to use of the internet and related technologies, and how these relate to children and young people, refreshing this knowledge on a regular basis.

IT Department:

- To report any E-Safety related issues that arise, to the E-Safety officer.
- To ensure that users may only access the school's networks through an authorized and properly enforced password protection policy.
- To ensure that provision exists for misuse detection and malicious attack, e.g. keeping virus protection up to date
- To ensure the security of the school ICT system
- To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices
- The school's policy on web filtering is applied and updated on a regular basis
- That he / she keeps up to date with the school's E-Safety policy and technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant
- That the use of the network / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Officer / SLTs for investigation / action / sanction
- To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a critical incident or system failure
- To keep up-to-date documentation of the school's e-security and technical procedures

All Staff:

- To read, understand and help promote the school's E-Safety policies and guidance
- To read, understand and adhere to the school staff Acceptable Use Agreement / Policy
- To report any suspected misuse or problem to the E-Safety officer
- To model safe, responsible and professional behaviours in their own use of technology
- Never upload any images of students or others without permission of parents or Staff
- To ensure that any digital communications with students should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones, social networking sites, etc.

Teachers :

- Educate students about appropriate and safe internet usage, including interaction and communication with other people on social networking websites and in chat rooms

- Encourage awareness about cyber bullying and give clear guidelines as to the steps that are to be taken and people that can be approached
- Monitor and ensure that there is no misuse of internet
- Raise awareness about the advantages and disadvantages of using Social media
- Use the online web-based interactive communication technologies to enhance students' education and learning and to facilitate collaborative study habits in students
- Improve peer collaboration and sharing of internet resources through sustained usage of online web-based interactive communication
- Share outstanding teaching practices through electronic communication
- Incorporate ICT in all areas of the curriculum to encourage the holistic approach of the students
- Develop the presentation skills using ICT for project work and competitions

Students

- Ensure they do not divulge any information about themselves or other persons on social media or through any other form of electronic communications over the Internet
- Not disclose their personal information
- Never upload any images of themselves or others without permission of parents or Staff
- Not Plan or arrange appointments with anyone they have met on the Internet
- Take proper measures if they receive any message that is inappropriate or makes them feel uncomfortable. They should immediately inform an adult they trust
- Ensure they are not exposed to information or images that might harm them or cause them discomfort
- Speak out against cyber bullying and immediately get in touch with the relevant Staff or parents
- Avoid trying to access websites that have inappropriate content and are restricted
- Not damage computers, computer systems, software, or computer networks
- Respect themselves and all other users through good network etiquette
- Say no to plagiarism and give due credit to anyone whose work they are using for educational purposes
- Help in raising awareness across School of acceptable and smart use of internet

Parents/ Guardians:

- Monitor and enforce their own family values to their children making them aware of the importance of using internet safely
- Involve their children in regular discussions regarding the different challenges that are presented through the internet
- Ensure that the children are aware of the acceptable internet discipline and the consequences if the rules are broken
- Maintain clarity and consistency on what is permissible and what activities are unacceptable
- Assume complete responsibility for monitoring their children's use of internet at home and outside School
- Have complete awareness of cyber bullying and ensure that the children are not being subjected to it in any form through monitoring and discussions
- Inform and work with the School if any misuse is reported or found
- Seek help and support from the School in case of any incident that involves cyber bullying
- Be well informed about the work or projects given to the children to rule out any misuse.

Cyber Bullying

The school will do the following as a minimum to impose a comprehensive and effective prevention strategy:
Ensure that all incidents of threats and cyber bullying both inside and outside school are dealt with immediately and will be managed and/or escalated in line with the procedures set out in the school's *Cyber-Bullying Policy.*

- Ensure that all staff know that they need to report any issues concerning cyber bullying
- Ensure that all staffs are aware of the Prevent Duties.
- Ensure that parents/Guardians are informed and attention is drawn to the E-Safety policy so that they are fully aware of the school's responsibility relating to safeguarding students against cyber-bullying.

E-Safety Officer and Student Behaviour Management Committee will

- Take overall responsibility for the co-ordination and implementation of cyber-bullying prevention and response strategies.
- Ensure that all incidents of cyber threats/bullying both inside and outside school are dealt with immediately and will be managed and/or escalated in line with the procedures set out in the school's, National Child Protection Policy in Educational Institutions in United Arab Emirates, *Behaviour Policy, Behaviour Management Policy-MOE, Behaviour Policy for Distance Learning-MOE, the Child Protection Policy, the Anti-Bullying Policy and Cyber-Bullying Policy.*
- Ensure that all staff knows that they need to report any issues concerning cyber threats/bullying.
- Ensure that the Safeguarding and Cyber-Safety Policy is available at all times on the school website.

The IT Support will

- Ensure adequate safeguards are in place to filter and monitor inappropriate content and alert the Student Behaviour management Committee to safeguarding issues.

Guidance for Staff

Guidance on safe practice in the use of electronic communications and storage of images is contained in the E-Safety Policy.
If you suspect or are told about a cyber-safety/ bullying incident, follow the protocol outlined below:

- Ask the student to save the material
- Print off the offending material straight away
- Inform the E-Safety Officer or the Student Behaviour management Committee and pass them the information that you have

Guidance for Students

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

- 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
- Do not give out personal details or contact information without the permission of a parent/guardian
- The school will deal with cyber bullying in the same way as other bullying. Do not think that because it is online it is different to other forms of bullying.

Guidance for Parents/Guardians

- Parents/Guardians can help by making sure their child understands the school's policy.
- Parents/Guardians should also explain to their children legal issues relating to cyber-safety/cyber-bullying.
- If parents/Guardians believe their child is the victim of cyber-bullying, they should save the offending material and make sure they have all relevant information before deleting anything.

- Parents/Guardians should contact the school as soon as possible.

Social Media Policy

This policy sets out a framework of good practice that students, staff and the wider community are expected to follow when using social media.

This policy covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of the school.

General Statement:

- Under no circumstances may the school's logos or brand be used or published on any personal web space or on any online or offline medium without prior consent
- Users should be conscious at all times of the need to keep their personal and professional/school lives separate.
- Users should not engage in activities involving social media which might bring the school into disrepute;
- Users should not represent their personal views as those of Leaders Private School on any social medium eg. Facebook, WhatsApp Groups
- Users should not discuss personal information about other students, School and the wider community they interact with on any social media;
- Users should not use social media and the internet in any way to attack, insult, abuse or defame students, their family members, colleagues, other professionals, other organisations or the School
- Students should only use official school sites for communicating with staff, or with other students to communicate with one another for the purposes of an educational context.
- Google Docs, School Website, MS Teams, Zoom, SEESAW are the current platforms by which staff and students should communicate and no other medium should be used without careful consideration.
- Social media websites like Facebook, Whatsapp and Instagram are filtered and restricted within the school premise for all users, except for the Principal, SLTs and IT Department.
- The school is responsible for running its official website and pages. No other social media platforms may be set up by any member of the whole school community which have a direct or indirect connection with School.
- The IT Manager will be responsible for Publishing Materials on the Schools Social Media.
- The IT Manger will Monitor and Manage the comment section of the Materials shared on the Schools' Social media.

Students: Social Media Guidelines:

- In the online environment, students must follow the School's Code of Conduct and conduct themselves online as in School.
- Think before you post.
- Leaders Private School reserves the right to request school-related images or content posted without permission to be removed from the internet.
- Do not misrepresent yourself by using someone else's identity.
- 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.
- 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.
- When responding to others, remember to be respectful and avoid comments that may be hurtful. Do not use profane, obscene, or threatening language.
- 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.

- 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 on unsecure sites.
- 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.
- Cyberbullying is considered an act of harassment.
- If you wish to promote a specific News, Activity or event organized by the school, you may do so only by means of a link to the official School Facebook account, Instagram Account, Twitter account, or YouTube channel.

Parent Social Media Guidelines:

- Parents are required to adhere to the following guidelines:
- Parents should expect communication from teachers prior to their child's involvement in any project using online social media applications.
- Parents will not attempt to destroy or harm any information online.
- Parents will not use classroom social media sites for any illegal activity, including violation of data privacy laws.
- Parents are highly encouraged to read and/or participate in social media.
- Parents should not distribute any information that might be deemed personal about the School.
- Parents should not upload or include any information that does not meet the Student Guidelines.

Social Media Guidelines for Faculty & Staff:

- All staffs 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.
- Your online behavior should reflect the same standards of honesty, respect, and consideration that you use face-to-face.
- Remember that social media used for education are an extension of your classroom. What is inappropriate in your classroom should be deemed inappropriate online.
- When contributing online do not post confidential student information.
- Before posting photographs and videos, permission should be sought from the subject where possible. This is especially the case where photographs of students and professional colleagues are concerned.
- If you wish to promote a specific News, Activity or event organized by the school, you may do so only by means of a link to the official School Facebook account, Instagram Account, Twitter account, or YouTube channel.
- 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.
- Before posting personal photographs, thought should be given as to whether the images reflect on your professionalism.

Rules For Publishing Material Online (including images of students)

The schools website and social media are a valuable tool for sharing information and promoting students' achievements. We recognize the potential for abuse. Therefore, the following principles will always be considered:

- Photographs published on the website and social media that include students will be selected carefully and will comply with good practice guidance on the use of such images
- Written permission from parents/ guardians will be obtained before photographs of students are published on
- the school website
- Staff must not take photographs of students using their personal devices – all student photographs must be taken using the school's camera.

- Files must be appropriately named in accordance with these principles.
- Only images of students in suitable dress shall be used and group photographs are preferred in preference to individual photographs.
- Content should not infringe the intellectual property rights of others – copyright may apply to text, images, music or video that originate from other sources.
- Content should be polite and respect others.
- Material must be proofread by a member of the SLT before being published.
- When photos and videos of school events are permitted to be taken by parents and guardians, they will be asked not to publish them on any public area of the Internet, including social networking sites

Data Protection

To be read in conjunction to the schools Privacy Policy
The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for
- longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected
- without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Policy"
- Risk assessments are carried out
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear routines for the deletion and disposal of data
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- The person with overall responsibility for compliance with the Act is the Data Protection Officer or DPO. All queries concerning data protection matters should be raised with the Data Protection Officer.

Communications

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Staff and student's communication should therefore use only the school email service to communicate with others.
- Users must immediately report, to the E-Safety officer, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and students or parents / guardian (email) must be professional in
- tone and content.
- These communications may only take place on official (monitored) school systems.
- Personal email addresses, text messaging or social media must not be used for these communications
- Students should be taught strategies to deal with inappropriate communications and be reminded of the need
- to communicate appropriately when using digital technologies
- Personal information should not be posted on the school website and only official email addresses should be
- used to identify members of staff.
- School must enable security measures to ensure that private communications do not take place in the Virtual Learning Environment.

Technology Platforms

The teachers will use appropriate platforms for each year/grade level groups for effective distance learning. Some of the key platforms being used are: -

KG, Grade 1 & 2

1. Zoom – to facilitate online synchronous learning, discussions and meetings
2. Seesaw - enables teachers to share content, distribute assignments, and manage communication with students, colleagues, and parents
3. Quizzes- for assessment

Primary and Middle

1. Zoom – to facilitate online synchronous learning, discussions and meetings
2. Microsoft Office 365 Teams – to facilitate online (asynchronous) discussions, meetings and sharing of resources distribute quizzes, assignments, and manage communication with students
3. NearPod, Mentimeter, Classroomscreen & Mindmiester– Student engagement platform where teacher can create presentations that can contain quizzes, polls, videos, images, drawing-boards, web content and so on
4. Quizzes, Kahoot, MS Forms, Google Forms – for assessment

Senior

1. Zoom – to facilitate online synchronous learning, discussions and meetings
2. Microsoft Office 365 Teams – to facilitate online (asynchronous) discussions, meetings and sharing of resources distribute quizzes, assignments, and manage communication with students
3. NearPod, Mentimeter, Classroomscreen & Mindmiester– Student engagement platform where teacher can create presentations that can contain quizzes, polls, videos, images, drawing-boards, web content and so on
4. Quizzes, Kahoot, MS Forms, Google Forms – for assessment
5. OLAB – for virtual lab practice

** New technologies shall be introduced as and when necessary after the verification and approval from the E-Safety officer.

Password Policy

A safe and secure password system is essential and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment.

- All school networks and systems will be protected by secure passwords that are regularly changed.
- Passwords for new users (including staff and students) will be allocated by the IT team.
- All users will have responsibility for the security of their username and password, must not allow other users to access the systems using their log in details and must immediately report any suspicion or evidence that there has been a breach of security.
- 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 90 days.
- Passwords must NOT be inserted into email messages or other forms of electronic communication.
- If forgotten, password can be reset by the IT team upon formal request.

All passwords will meet the following criteria:

- 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 personal information, names of family, etc.

Do Not:

- reveal a password over the phone to ANYONE.
- reveal a password in an email message.
- reveal a password to a supervisor.
- talk about a password in front of others.
- hint at the format of a password (e.g., "my family name").
- reveal a password on questionnaires or security forms.
- share a password with family members.
- reveal a password to co-workers.
- reveal a password to vendors.
- In short, don't reveal a password to ANYONE.
- use the "Remember Password" feature of applications.
- write passwords down and store them anywhere in your office.
- store passwords in a file on ANY computer.

Filtering Policy

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.
This policy sets out the principles to maintain and support research, teaching and other management activities whilst protecting users, networks and computers from hostile or unwanted network traffic and illegal or other content
This policy covers all employees, students, Governors, consultants, contractors, volunteers and agency staff working for the School.

Policy:

- Through the use of firewall and web filtering technologies, the school prevents access to certain categories of websites via its networks.
- The School does this to protect its users, networks and computers from accessing illegal or other content that would either be unlawful and/or in breach of the regulations of the school
- The current Content Classification System provided through the firewall vendor allows for site blocking based on a range of categories e.g. 'Adult', 'Hacking', 'Extremism'
- Access to Social Media websites are prevented by the firewall.
- The school systems are installed with Antivirus and protected from Virus and Malicious Programs.
- The school reserves the right at any time to amend, add or delete categories that are blocked under this Policy
- In the interests of academic freedom, and for legitimate research, teaching and learning purposes, it is recognised that staff and students may require access to sites which are currently blocked.
- The School has a 'whitelisting' process to enable staff and students with legitimate requests to be granted access to websites and online material which have been blocked under this Policy and through the content filtering technologies in force for the duration of their research.

- A Whitelisting Request can be raised with the school's IT Team via email.

Fortiguard Web Filtering

The school uses a firewall application- "Fortiguard" to block dangerous or undesirable websites and protocols.

Each time a request to a website or app is made, Fortiguard intercepts the DNS request (the lookup address for the domain name). It then checks this DNS record against the blocklist. If the site is blocked, it will block the DNS request and the website cannot be reached.

The school has enabled category based blocking and blacklisting of websites and if required the school will enable keyword based blocking.

Users are divided into 2 categories: 'Staff and Non-Teaching Staff' and 'Student'. Their access rights will depend on their username.

Requesting Change

Web Filtering is an on-going process and will need amending from time to time.
The process for requesting change in web filtering.

1. If a site has been incorrectly blocked please contact the IT Dept with the URL of the web page and the message displayed on screen.
   If after a review the site is deemed to be incorrectly categorized then IT Dept will endeavour to re-categorize.

2. If correctly categorized, then the request will be forwarded to the schools E-Safety Officer to alter the filtering policy.

Network and Internet Access

The school can determine who gets permission to access the Internet. It is recommended that all members have Internet Access and that they have an appropriate level of Internet filtering assigned to them. This means that there is an auditable trail on their Internet access.

All users who have access to the school managed service system must sign an Acceptable Use Agreement indicating that they understand what is meant by Safe and Responsible Use of the Internet.

- The schools Internet access is regulated based on users in firewall.
- Only the school's staffs can access the internet at all times
- Students, if required, shall access the internet only through the designated systems provided in the computer lab with prior permission from a member of the SLT and they will be supervised at all times.
- Visitor are not allowed to access the School's Wi-Fi.
- Networked folders are accessible only by the school staffs
- The networked folders share rights are managed and configured by the IT Department.

Use of Mobile Device

- Students are not allowed to bring their own Mobile devices to school at all times, unless informed by the school.
- The use of devices for students are restricted to the computer labs only and will be monitored at all times.

- All Staffs may have the opportunity to use their personal electronic devices for work purposes.
- To ensure the security, all staffs are required to have anti-virus and mobile device management (MDM) software installed on their personal mobile devices
- Personal devices should be turned off or set to silent or vibrate mode during classes, meetings and conferences and in other locations where incoming calls may disrupt normal workflow.
- While at work, all staffs are expected to exercise the same discretion in using their personal devices as is expected for the use of company devices.
- Staff and students agree to only view, listen to, or access, school appropriate content on their personal devices while at school.
- While using the IT resources of the school all users must comply to the IT policy set by the school.
- The school's IT Team reserves the right to refuse the connection of personal devices to the School network if such equipment is being used in any way that could potentially cause harm to the school's systems, data, users or resources.

Reporting E-Safety Incidents

Students:

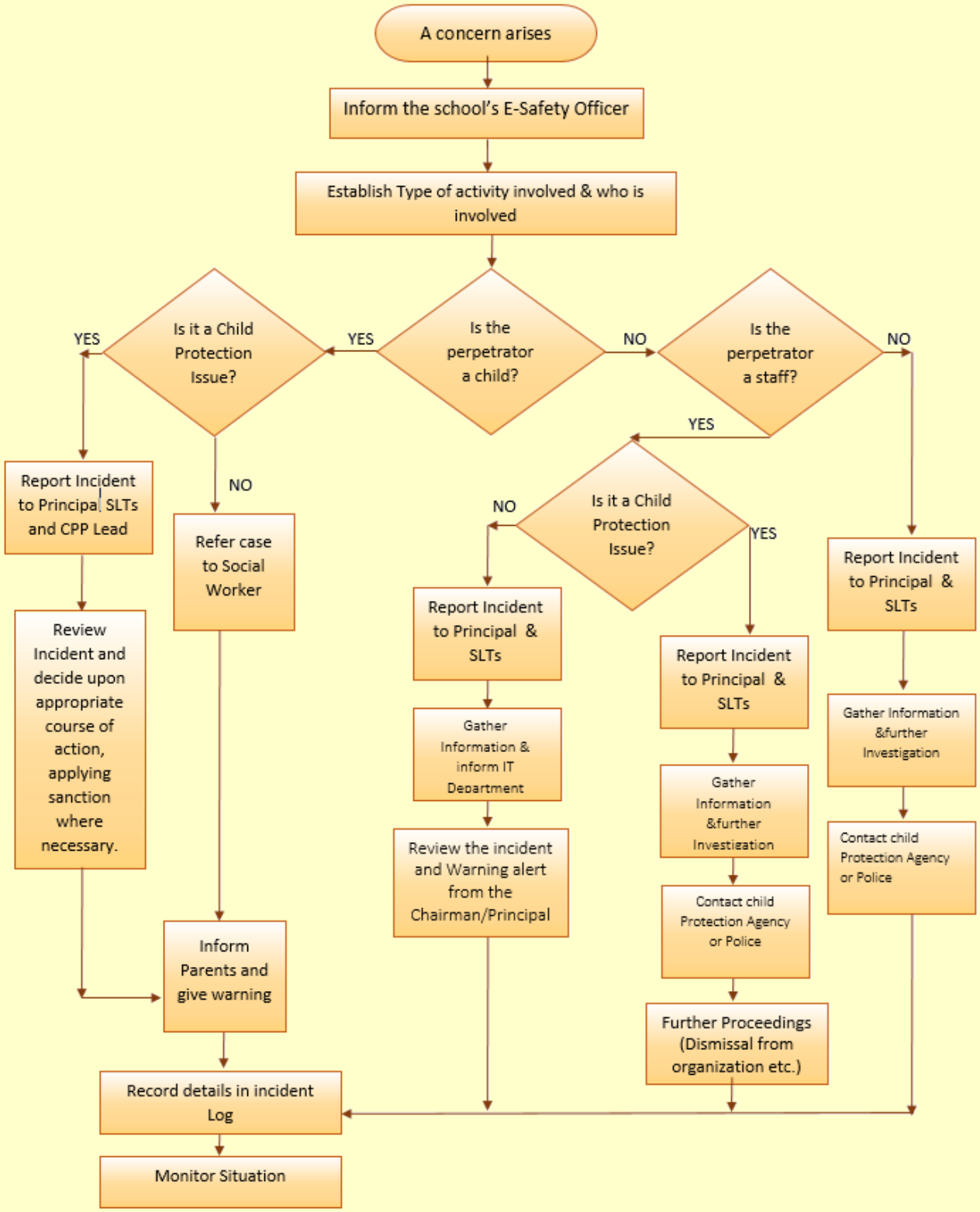
- Should speak to any member of staff they trust of anything that has made them feel uneasy or having accessed anything they may consider indecent or inappropriate.
- They may use appropriate online channel provided by the school to report an incident- Through mail (ursafe@leadersprivateschool.com), through phone(06 5225560 Ext 122) , Informing a trusted staff or by the facility of reporting an incident anonymously through the school website.

The member of staff should:

- Report any incident informed by the student, parent / guardians to the E-Safety Officer immediately
- Report any incident observed to the E-Safety Officer immediately
- Preserve any evidence related to the offense and submit it to the E-Safety Officer

Responding to an Incident

Flowchart for responding to e-safety incidents in school.



Disciplinary Procedure

School Procedures Following Misuse by Student:
In the event that an incident is reported against a student, the matter will be analysed and the offenses will be dealt with as per the guidelines set in the National Child Protection Policy in Educational Institutions in United Arab Emirates ,*Behaviour Policy, Behaviour Management Policy-MOE, Behaviour Policy for Distance Learning-MOE, the Child Protection Policy, the Anti-Bullying Policy and Cyber-Bullying Policy*

School Procedures Following Misuse by Staff:
In the event that a member of staff is believed to misuse the Internet or E-learning platforms in an abusive or illegal manner, it will be reported to the E-Safety Officer and Senior Leadership Team immediately. Violations of these policies may incur the same types of disciplinary measures and consequences as violations of other School policies, including progressive discipline up to and including termination of employment.
In some cases, violations of this policy may also be violations of Government laws, and consequences may include criminal prosecution.

All staff must follows these procedures, in the event of any misuse of the Internet:
A. An inappropriate website is accessed inadvertently:

- Report website to the E-Safety Officer who will inform the IT Teams and ensure that it be added to the banned or restricted list.

B. An adult receives inappropriate material.

- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the E-Safety Officer immediately.
- E-Safety Officer will ensure the device is removed and log the nature of the material. Inform IT team as in A.

C. An inappropriate website is accessed deliberately.
The person discovering this must:

- Ensure that no one else can access the material.
- Report to the E-Safety Officer immediately. The E-Safety Officer will refer back to the E-Safety Policy and follow agreed actions for discipline. He/She will inform the IT team to update the filtering service.

D. An adult has used ICT equipment inappropriately:

- Follow the procedures for C.

E. An adult has communicated with a student inappropriately or used ICT equipment inappropriately.
The person discovering this must:

- Ensure the student is reassured and remove them from the situation immediately, if necessary.
- Preserve the information received by the student if possible and determine whether the information received is abusive, threatening or innocent.
- If illegal or inappropriate misuse is known, contact the Senior Leadership Team and E-Safety Officer immediately and follow the Child Protection Policy.

F. Threatening or malicious comments are posted to the school website or any other platform about a student or an adult in school:

- Preserve any evidence.
- Inform the Senior Leadership Team and E-Safety Officer as necessary, who will then refer back to the E-Safety Policy and follow agreed actions for discipline.

Schedule for Monitoring and Reviewing of E-Safety Policy

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to E-Safety or incidents that have taken place.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys of reported incidents:
    - Students
    - Parents / Caregivers
    - Staff