CPS ONLINE SAFETY POLICY

Schedule Development/Monitoring/Review

This Online Safety Policy was approved by the Governing Body on the 25th of December 2020. Implementation of this Online Safety Policy will be monitored by the Online Safety Leader, Online Safety Coordinator.

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

The Governing Body will receive reports and/or updates on the implementation of the Online Safety Policy half-yearly generated by the Online Safety Coordinator.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs if internet activity
- Internal monitoring data for network activity
- Surveys of reported incidents
    - Students
    - Parents/Caregivers
    - Staff

Scope of the Policy

This policy applies to all members of the Crown Private School who have access to and are users of the school ICT systems, both in and out (remote) the school:

- Staff
- Students
- Volunteers
- Parents/guardians
- Contractors
- Community Users

The Governing Body asks the Principal of Crown Private School to such extent as is reasonable, to regulate the behavior of students when they are off the school site and asks members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

Crown Private School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / caregivers of incidents of inappropriateonline safety behaviour that take place out of school.

Roles and Responsibilities

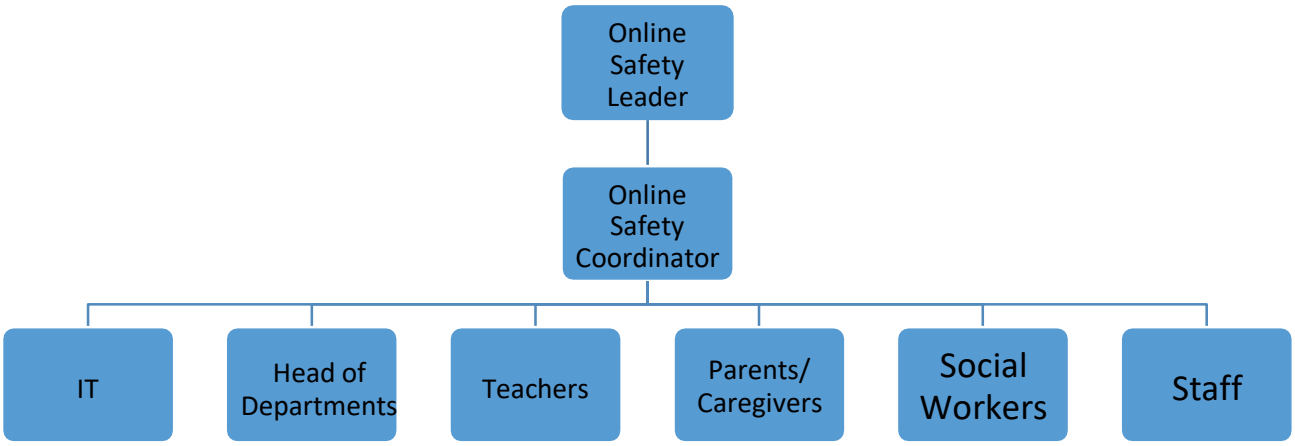
This outlines the Online Safety roles and responsibilities of individuals and groups within the school:

Governing Body:

governing body are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the governing body receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of the Online Safety Leader. The role of the Online Safety Leader will include:

- Regular meetings with the Online Safety Coordinator
- Regular monitoring of Online Safety incident logs
- Regular monitoring of filtering/change control logs
- Reporting to relevant governing body/Board/Committee on appropriate matters

Crown Private School Online Safety Group



Online Safety Leader	**Principal**	**Dr. Kishor Pillai**
Online Safety Coordinator	**Vice Principal**	**Ms. Flavia Castelino**
IT	IT Administrator Facilities Manager	Mr. Rajeesh Kumar Mr . Gokul Ajith
Head of Departments	Teaching and Learning Assessment & Administration EYFS Primary English Mathematics Science ICT	Ms. Flavia Castelino,Laed Vice Principal Ms. Stephaine Orrell, Head of KG Ms. Lalita Karasi (Vice principal Primary) Mr. Ahmed Kharwa Ms. Janani Rao Mr. Vinith Pillai Ms. Dhanya Ravindran
Child Protection and Well being	Social Worker Psychologist SENCo Supervisor	Ms. Ihsan Salim Ms. TeenahM Mr. Kevin Oliver and Ms Venera Golubina Ms. Eman Al Haj
Parents/Caregivers	Parents Council	Representatives for each class
Teachers		All Teachers (Homeroom and Subject)
Staff		All Staff (including admin)

Online Safety Leader, Dr. Kishor Pillai, Principal

- The Principal has a duty of care for ensuring the Safety (including Online Safety) of members of the Crown Private School Community.
- The Principal and (at least) another member of the Senior Leadership Team (in this case it is the Online Safety Coordinator) should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Online Safety Leader will take daily reports from the Online Safety Coordinator, the Social Worker, School Nurse, the school HR manager to ensure that all children in school and those online are safe and secure as per the child protection policy.
- The Online Safety Leader and the Online Safety Coordinator are responsible for ensuring that staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles including himself

Online Safety Coordinator, Mr. Flavia Castelino, Vice Principal

- Leads the Online Safety Group
- Takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place
- Provides training and advice for staff
- Liaises with the Ministry of Education / relevant body
- Liaises with school technical staff
- Receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments
- Meets regularly with Online Safety Leader to discuss current issues, review incident logs and filtering /change control logs
- Attends relevant meeting / committee of the Governing Body.
- Reports regularly to the Governing Body.

IT Administrator, Mr. Rajeesh

Facilities Manager, Mr. Gokul

The IT Administrator & Facilities Manager is responsible to ensure

- That the school's technical infrastructure is operational, secure and is not open to misuse or malicious attack
- That the school meets required Online Safety technical requirements and any Ministry of Education / other relevant body Online Safety Policy / guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- The filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- That they keep up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant
- That the use of the network / internet / remote access / ERP/LMS/ email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online SafetyLeader and Coordinator

Head of Departments, Teachers, Support Staff

- They have an up to date awareness of online safety matters and of the current school
- Online safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- They report any suspected misuse or problem to the IT Administrator and/or the Online Safety Coordinator for investigation / action / sanction
- They ensure all digital communications with students / parents / Guardians should be on aprofessional level and only carried out using official school systems
- Online Safety issues are embedded in all aspects of the curriculum and other activities
- Students understand and follow the online safety and acceptable use policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Social Workers

- Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
    - Sharing of private and personal data
    - Access to illegal / inappropriate materials
    - Inappropriate on-line contact with adults / strangers
    - Potential or actual incidents of grooming
- To ensure to train all staff and to make sure that they are aware of Child protection/safeguarding (as mentioned above).

Students:

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realize that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school
- Mobile Phones and Wearable Technologies – Students should not be in possession of mobile phones or any other wearable technologies with cellular capability.

Parents / Caregivers:

- Parents / Caregivers play a crucial role in ensuring that their children understand the need to use the internet /mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local Online Safety campaigns / literature. Parents and caregivers will be encouraged to support the school in promoting good Online Safety practice and to follow guidelines on the appropriate use of:
    - Digital and video images taken at school events
    - Access to parents' sections of the website
    - Their children's personal devices in the school (where this is allowed)

Contractors/ Visitors

Key responsibilities:

- Report any concerns, no matter how small, to the designated safeguarding lead / online safety coordinator.
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology

Policy Statements

Education

Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in Online Safety is therefore an essential part of the school's Online Safety provision. Children and young people, whether face-to-face or online (remote) need the help and support of the school to recognize and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / Moral Education/ other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Administrator (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

Parents / Caregivers

Many parents and Guardians have only a limited understanding of online safety risks and issues, yet theyplay an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and caregivers through:

- Curriculum activities
- Letters, newsletters, website

- Parents / Caregivers meetings
- High profile events / campaigns e.g. Safer Internet Day (09th February 2021)
- Reference to the relevant websites / publications

The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family useful information in use of new digital technologies, digital literacy and online Safety
- The school website will provide Online Safety information for the wider community

Education and Training

Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the Online Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify Online Safety as a training need within the performance management process
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Agreements
- The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events (e.g. from Local Authorities/Ministry and/or other relevant organisations) and by reviewing guidance documents released by relevant organisations
- This Online Safety policy and its updates will be presented to and discussed by staff in staff / team meetings /CPD days (Mondays)
- The Online Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

Training

Governing body

governing body should take part in Online Safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / Online Safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Ministry of Education or other relevant organisation
- Participation in school training / information sessions for staff

Technical

Network Infrastructure / Equipment, Filtering and Monitoring

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

- Filtering Policy
- Password Security policy
- Technical Security
- Protecting Personal information
- Acceptable Usage Policy

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of Online Safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- All the devices will be covered by the school's normal filtering systems,while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

Use of Digital Images and Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the

internet. However, staff, parents / caregivers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognize the risks attached to publishing their own images on the internet, e.g. on social networking sites
- Parents / caregivers are welcome to take videos and digital images of their children at school events for their own personal use . To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / Guardians comment on any activities involving other students / students in the digital / video images
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital / video images that students / students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images
- Students' full names and any other private information such as, EID, passport, etc, will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or guardians will be obtained before photographs of students are published on the school website. Parents/Guardians may withdraw permission, in writing, at any time.
- Students' work can only be published with the permission of the pupil and parents or Guardians

Data Protection (followed as guidelines)

UAE Federal law of 2012 and 2016 suggests that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and where necessary, up to date
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

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 Notice" and lawfully processed in accordance with the "Conditions for Processing".

Owners (Information Asset Owners)

- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

Staff must ensure that they:

- At all times take care to ensure the safekeeping of personal data, minimizing the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

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. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate for official purposes.
- Users must immediately report, to the nominated person – in accordance with the school / policy, 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 / caregivers' (email) must be professional in tone and content.

- Students should be taught about Online Safety issues, such as the risks attached to the sharing of personal details. They should also 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

Social Media - Protecting Professional Identity

The school provides the following measures to ensure reasonable steps are in place to minimize risk of harm to students, staff and the school through limiting access to personal information:

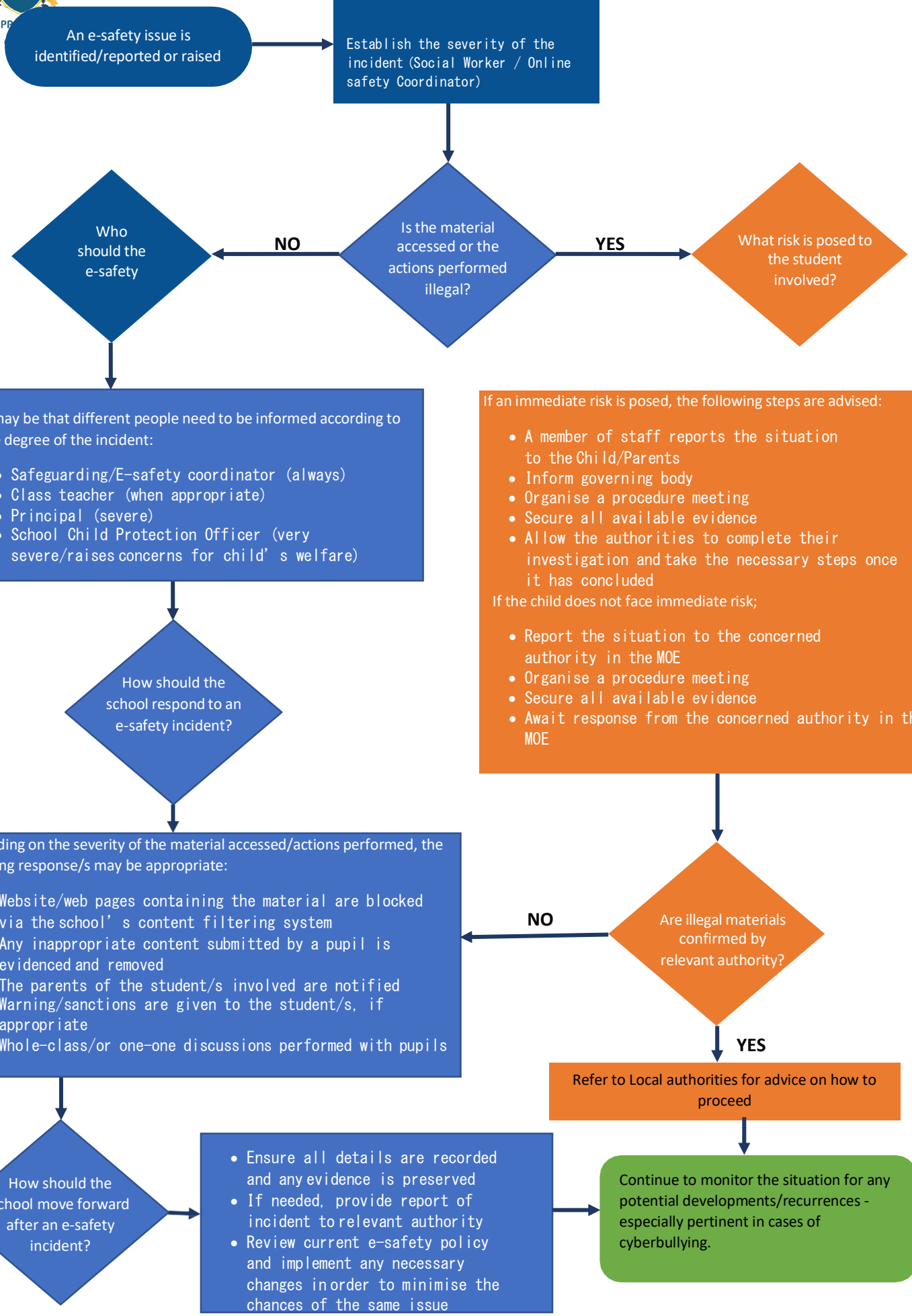
- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students, parents / caregivers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or Ministry of Education
- Security settings on personal social media profiles are regularly checked to minimize risk of loss of personal information
- The school's use of social media for professional purposes will be checked regularly by the Online safety coordinator and Online Safety to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Handling Online Safety complaints/incidents

online	**LINK**: online form link is available on our school website which can be accessible at any time for students, parents and or staff can log in their complaints, issues or comments which will reach the social worker and will get back to you promptly. Options of anonymous reporting is available
Inschool	**WORRY BOX/SUGGESTION BOX** A Box is placed near the reception area in our school where, students, parents or staffs can put their complaints, issues and comments which will reach our social worker and will get back to you promptly. options of anonymous reporting are available.
Online video conference	**Zoom Link: https://zoom.us/j/9434435899?pwd=QkRVbGpsZldHK2o0em8za3JNdnNhdz09** **Meeting ID: 943 443 5899 Passcode: crown123** This is a recurring meeting from 7.30 am - 3.00 pm
Phone	We have a dedicated Parent Complaint Officer with a four-member team looking into staff/student wellbeing Please call **056 358 6249** to resolve any queries you may have.


An e-safety issue is identified/reported or raised
Establish the severity of the incident (Social Worker / Online safety Coordinator)
Is the material accessed or the actions performed illegal?
NO
YES
Who should the e-safety
What risk is posed to the student involved?
It may be that different people need to be informed according to the degree of the incident:
Safeguarding/E-safety coordinator (always)
Class teacher (when appropriate)
Principal (severe)
School Child Protection Officer (very severe/raises concerns for child's welfare)
How should the school respond to an e-safety incident?
If an immediate risk is posed, the following steps are advised:
A member of staff reports the situation to the Child/Parents
Inform governing body
Organise a procedure meeting
Secure all available evidence
Allow the authorities to complete their investigation and take the necessary steps once it has concluded
If the child does not face immediate risk;
Report the situation to the concerned authority in the MOE
Organise a procedure meeting
Secure all available evidence
Await response from the concerned authority in the MOE
Depending on the severity of the material accessed/actions performed, the following response/s may be appropriate:
Website/web pages containing the material are blocked via the school's content filtering system
Any inappropriate content submitted by a pupil is evidenced and removed
The parents of the student/s involved are notified
Warning/sanctions are given to the student/s, if appropriate
Whole-class/or one-one discussions performed with pupils
Are illegal materials confirmed by relevant authority?
NO
YES
Refer to Local authorities for advice on how to proceed
How should the school move forward after an e-safety incident?
Ensure all details are recorded and any evidence is preserved
If needed, provide report of incident to relevant authority
Review current e-safety policy and implement any necessary changes in order to minimise the chances of the same issue
Continue to monitor the situation for any potential developments/recurrences - especially pertinent in cases of cyberbullying.

School Actions & Sanctions

- It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

Violations / Unacceptable use of Policies

Severity of violation	For Student	For Staff
LOW (Does not cause issues to others or the system)	• Written Warning • letter to the parent • confiscation of device • Taking away privilege	• Written warning/ Explanation • Recorded into performance evaluation system
MEDIUM (Causing temporary inconvenience to others or the system)	• Written Warning • letter to the parent • confiscation of device • Temporary suspension from school activity	• Written Warning • letter to the parent • confiscation of device • Same device or privileges or access right will be revoked
HIGH (Causing permanent/ serious damage to others or system	• Written Warning • letter to the parent • confiscation of device • Report to relevant local authorities • Suspension until issue resolved.	• Written Warning • letter to the parent • confiscation of device • Report to relevant local authorities • Termination of contract with immediate effect

*Violations as per the UAE safety regulations will be treated as per the law.

* Any third violation at level 1 or level 2 will be result in moving the level up

Updated by	Last reviewed	Anticipated Review Date
Ms. Flavia Castelino (Online Safety Coordinator) Mr. Rajeesh Kumar, (IT Administrator)	20 – SEP- 2022	20- JAN -2023