Online Safety Policy

Brilliant International Private School

Academic Term 2020 – 2021

Contents

Development/Monitoring/Review of this Policy

This online safety policy has been developed by the E-Safety team made up of:

- Ms. Makala Cooper (E-Safety Safety Coordinator)
- Mr. Yasir Karukunnathu (IT Support – Executive)
- Ms. Lleranie Tahir (KG Teacher)
- Ms. Maha Awad (Primary Teacher)
- Ms. Lynda Arinde (Secondary Teacher)
- Mr. Mohammed Khalaf (Secondary Boys Supervisor - Behaviour)
- Mr. Ajeeb Abbas (Boys Counsellor – Well Being)
- Ms. Sara (Girls Counsellor – Child Protection & Safeguarding)
- Ms. Nazna Mustafa (Parental Communication)

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Board of Directors:	Date to be added.
The implementation of this online safety policy will be monitored by the:	E-Safety Co-ordinator
Monitoring will take place at regular intervals:	Termly
The Board of Directors will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Termly
The online 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 online safety or incidents that have taken place. The next anticipated review date will be:	June 2020
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Police 999 (8002626) MOI. http://www.moi-cpc.ae/en/CONTACT.US.aspx

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of
    - Pupils
    - Parents
    - Staff

Scope of the Policy

This policy applies to all members of the school community (including staff, students, parents, visitors,) who have access to and are users of school digital technology systems, both in and out of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

Board of Directors

Directors 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 Directors receiving regular information about online safety incidents and monitoring reports.

Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the E-Safety Coordinator.
- The Headteacher and Vice Principal have clear procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Principal and Senior Leaders are responsible for ensuring that the E-Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal and Senior Leaders 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.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Coordinator.

Online Safety Coordinator

- Leads the E-Safety team
- 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 SPEA.
- 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 Governor/Director to discuss current issues, review incident logs and filtering/change control logs
- Updates Directors on E-Safety within the school
- Reports regularly to Senior Leadership Team

Network Manager/Technical staff

Those with technical responsibilities are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and policy from the Khalifa Empowerment program.
- That users may only access the networks and devices through a properly enforced password protection policy.
- 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 networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Principal and Senior Leaders; Online Safety Lead for investigation/actions.
- That monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school/academy online safety policy and practices
- They have read, understood and signed the staff acceptable use agreement.
- They report any suspected misuse or problem to the E-Safety Coordinator for investigation/actions.
- All digital communications with students/parents should be on a professional level and only carried out using official school systems (BIPs Application, School email).
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Students understand and follow the Online Safety Policy 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.

Designated Safeguarding Person

Has received training in online safety issues and is aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

E-Safety Team

The E-Safety Team provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives.

Members of the E-Safety Team assist the E-Safety Coordinator with:

- The production/review/monitoring of the school online safety policy/documents.
- The production/review/monitoring of the school filtering system and requests for filtering changes.
- Mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression.
- Monitoring network/internet/filtering/incident logs
- Consulting stakeholders – including parents and the students about the online safety provision.
- Monitoring improvement actions identified through Adqar eSafe school programme.

Students/Pupils:

- Are responsible for using the school digital technology systems in accordance with the student acceptable use agreement.
- 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 laws of the UAE. They should also know and understand policies on the taking/use of images and on online-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school

Parents/carers

Parents 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 parental conference sessions, BIPs application, circulars, website, social media and information about Federal online safety campaigns. Parents 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 or on online.
- Access to Learning Platform.
- Their children's personal devices in the school.

Community Users

Community Users who access school systems or programmes as part of the wider school provision will be expected to sign a Community User agreement before being provided with access to school systems.

Policy Statements

Education – Students/Pupils

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/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise 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 ICT 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/pupils should be supported in building resilience by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students should be helped to understand the need for the student 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, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff 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.

Education – Parents/carers

Many parents have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online 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/academy will therefore seek to provide information and awareness to parents through:

- Curriculum activities
- Circulars, website, Learning Platform
- Parents sessions
- High profile events/campaigns e.g. Microsoft E-Safety Day
- Reference to the relevant web sites/publications e.g. https://saferinternetday.ae

Education – The Wider Community

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

- Providing family learning courses in use of new digital technologies, digital literacy and online safety.
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community.
- Sharing their online safety expertise/good practice with other local schools.

Education & Training – Staff

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 planned 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.
- 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.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- This online safety policy and its updates will be presented to and discussed by staff in staff meetings/training sessions.
- The E-Safety Coordinator will provide advice/guidance/training to individuals as required.

Training – Directors

Directors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided at a Federal Level or through SPEA.
- Participation in school information sessions for staff or parents.

Technical – infrastructure/equipment, filtering and monitoring

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and are requested to change their secure password on first login. Users are responsible for the security of their username and password.
- The "administrator" passwords for the school systems, used by the IT Executive must also be available to the Principal or other nominated senior leader and kept in a secure place.
- The IT Executive is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list.

Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.

- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced/differentiated user-level filtering.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place that a/forbids staff from downloading executable files and installing programmes on school devices.

Mobile Technologies (including BYOD)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

Students during their breaktime are not allowed to use devices and are expected to have non-screen time. This is for their own well-being and for them to interact with other students and staff within the room.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying 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 recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website/social media/local press.
- Staff 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 were possible should only be taken on school equipment; images on personal devices must be deleted.
- Care should be taken when taking digital/video images that 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 will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's work can only be published with the permission of the student and parents.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff				Students			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school.	X				X			
Use of mobile phones in lessons.		X					X	
Use of mobile phones in social time.	X							X
Taking photos on mobiles phones.		X					X	
Use of other mobile devices e.g. tablets.	X				X			
Use of personal email addresses within the school.				X			X	
Use of school email for personal emails.				X				X
Use of message apps.	X							X
Use of Social Media.				X				X
Use of blogs.				X				X

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

- The official school email service and BIPs application 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 with others when in school.
- 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 (email, social media, chat, blogs, etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging, WhatsApp or social media must not be used for these communications.
- 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

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools, could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school/academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published.
- Training is provided including: 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/academy staff should ensure that:

- No reference should be made in social media to students, parents 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.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

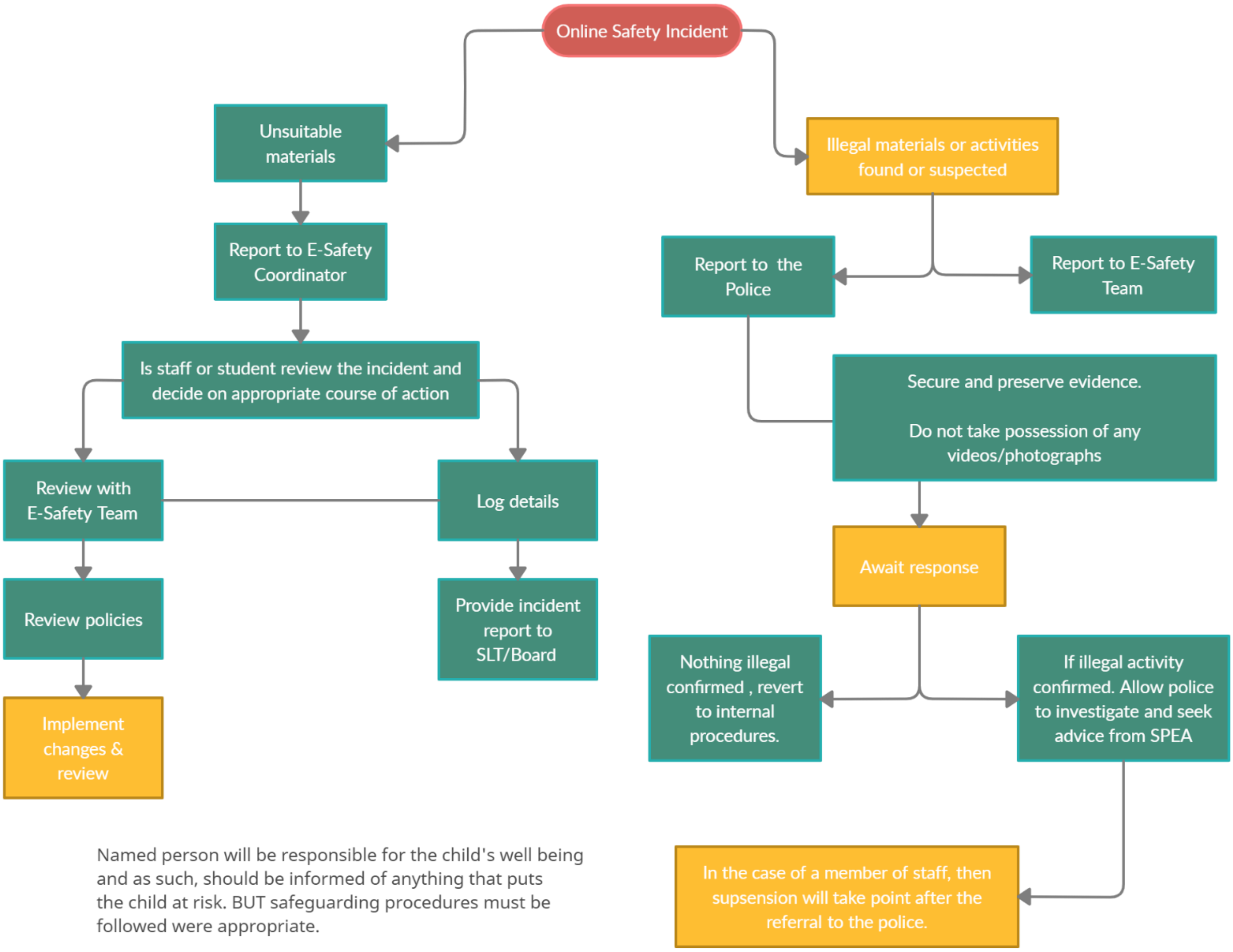
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school/academy when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate, or pass on material, remarks, proposals or comments that contain or relate to:	Child pornography - Article 29 of Federal Law No. 3 of 2016 Concerning Child Rights					X
	Impersonation, fraud and phishing.					X
	Insult, slander and defamation.					X
	Discrimination, racism and contempt of religion.					X
	Pornography				X	
	Threatening behaviour				X	
	Any other information which may be offensive to colleagues or brings the school in to disrepute.				X	
Activities that may be classed as cyber activities under the new Cyber crime law: • Accessing an electronic site illegally. • Medical related data. Distributing or altering. • Electronic card and bank account numbers. • Electronic communication. Intercept, capture without permission. • Gambling activities. • Human trafficking. • Terrorist activities. • Narcotics and money laundering.						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.					X	
Revealing or publicising confidential or proprietary information (e.g. personal information, computer/network access codes and passwords)					X	
Using school systems to run a private business					X	

Infringing copyright				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)				X	
On-line shopping/commerce				X	
Use of social media			X		
Use of messaging apps		X			
Use of video broadcasting e.g. Youtube		X			

Responding to incidents of misuse

This guidance is intended for use when staff 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.



Online Safety Incident
Unsuitable materials
Report to E-Safety Coordinator
Is staff or student review the incident and decide on appropriate course of action
Review with E-Safety Team
Log details
Review policies
Provide incident report to SLT/Board
Implement changes & review
Illegal materials or activities found or suspected
Report to the Police
Report to E-Safety Team
Secure and preserve evidence.
Do not take possession of any videos/photographs
Await response
Nothing illegal confirmed , revert to internal procedures.
If illegal activity confirmed. Allow police to investigate and seek advice from SPEA
In the case of a member of staff, then suspension will take point after the referral to the police.
Named person will be responsible for the child's well being and as such, should be informed of anything that puts the child at risk. BUT safeguarding procedures must be followed were appropriate.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by SPEA.
    - Police involvement and/or action.
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - Incidents of ‘grooming’ behaviour
    - The sending of obscene materials to a child
    - Criminally racist material
    - Promotion of terrorism or extremism
    - Offences under the Cybercrime act,
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

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. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

	Actions/Sanctions									
Students	Refer to class teacher/Homeroom	Refer to HOD	Refer to Supervisor	Refer to E-Safety Coordinator	Refer to Police	Refer to Principal	Refer to IT	Inform Parents	Warning	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal.				X	X	X		X		
Unauthorised use of non-educational sites during lessons										
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device										
Unauthorised/inappropriate use of social media/ messaging apps/personal email										
Allowing others to access school platform by sharing username and passwords										
Attempting to access or accessing the school platform, using another student's account										
Corrupting or destroying the data of other users										
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature										
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school										
Using proxy sites or other means to subvert the school's filtering system										
Accidentally accessing offensive or pornographic material and failing to report the incident										
Deliberately accessing or trying to access offensive or pornographic material										

	Actions/Sanctions								
Staff	Refer to Line Manager	Refer to Principal	Refer to SPEA	Refer to E-Safety Coordinator	Refer to Police	Refer to IT	Suspension	Warning	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal.		X	X	X	X				
Inappropriate personal use of the internet/social media/personal email									
Unauthorised downloading or uploading of files									
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account									
Careless use of personal data e.g. holding or transferring data in an insecure manner									
Deliberate actions to breach data protection or network security rules									
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software									
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature									
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students									
Actions which could compromise the staff member's professional standing									
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's filtering system									
Accidentally accessing offensive or pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material									