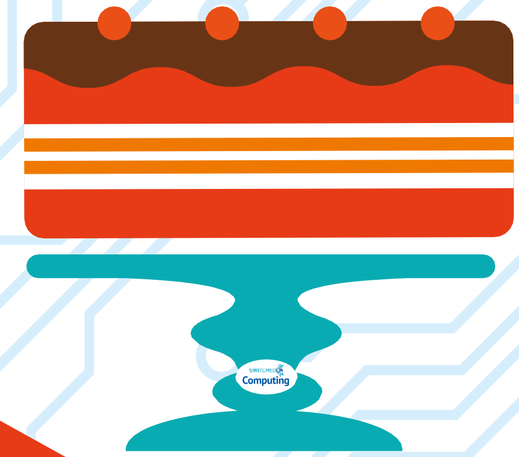
أكاديمية الفجيرة العلمية الإسلامية

Fujairah Islamic Scientific Academy

Risk of Internet
&
E – Safety Policy

A recipe for a safer internet



Be as kind to people online as you would be to them in the playground.

Keep personal information private; this includes your last name, Passwords, photos and School name.

Age

Check the age restrictions of games, apps and websites. You might not be old enough!

?

Only post photos or videos of people if you have asked their permission first.

Don't meet up. Meeting someone you have only spoken to online can be dangerous. Always check with an adult you trust.

Tell someone if you feel worried or uncomfortable about something.

Prepared by:
IT Department FISA School

e-Safety

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

Roles and Responsibilities:

The following section outlines the e-Safety roles and responsibilities of individuals and groups within the school:

Board of Directors:

Board of Directors are responsible for the approval of the *e-Safety* Policy and for reviewing the effectiveness of the policy.

Principal / Vice Principal:

- The ***Principal*** has a duty of care for ensuring the *e-Safety* of members of the school community, though the day to day responsibility for e-Safety may be delegated to the *e-Safety* Co-coordinator.
- The ***Principal*** and the ***Vice Principal*** are aware of the procedures to be followed in the event of a serious *e-Safety* allegation being made against a member of staff or to any of the student.
- The ***Principal*** is responsible for ensuring that the e-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their *e-Safety* roles and to train other colleagues, as relevant.
- The ***Principa***l will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal *e-Safety* monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

IT Administrator:

It is the responsibility of the school to ensure that the **IT Administrator / Technical staff** carries out all the e-Safety measures as suggested below:

It is also important that the **IT Administrator / Technical Staff** is fully aware of the school e-Safety policy and procedures.

The **IT Administrator / Technical Staff** is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets (as a minimum) the required e-Safety technical requirements as identified by the Local Authority or other relevant body and also the e-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.
- that the filtering policy, is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- that they keep up to date with e-Safety 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 / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the ***Principal*** and the ***Vice Principal***.

Teaching and Support Staff:

Are responsible for ensuring that:

- they have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices.
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement.
- they report any suspected misuse or problem to the ***Principal*** and the ***Vice Principal*** for investigation / action.
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems.
- e-Safety issues are embedded in all aspects of the curriculum and other activities.
- students / pupils understand and follow the e-Safety and acceptable use agreements / policies.
- in lessons where internet use is pre-planned students / pupils 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.

Students / pupils:

- are responsible for using the school digital technology systems in accordance with the Student / Pupil 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 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 e-Safety practice when using digital technologies out of school and realize that the school's e-Safety Policy covers their actions out of school.

Communications:

This is an area of rapidly developing technologies and uses. Schools will need to discuss and agree how they intend to implement and use these technologies e.g. few schools allow students / pupils to use mobile phones in lessons, while others identify educational potential and allow their use. This section may also be influenced by the age of the students / pupils. The table has been left blank for school to choose its own responses.

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 and Other Adults				Students			
Communication Technologies:	**Allowed**	**Allowed at certain times**	**Allowed for selected staff**	**Not allowed**	**Allowed**	**Allowed a certain times**	**Allowed with Staff permission**	**Not allowed**
Mobile phones may be brought to school	x							x
Use of mobile phones in lessons			x					x
Use of mobile phones in social time	x							x
Taking photos on mobile phones / cameras		x				x		x
Use of other mobile devices e.g. tablets.	x					x		x
Use of personal email addresses in school, or on school network		x						x
Use of school email for personal emails			x					x
Use of messaging apps			x					x
Use of social media			x					x
Use of blogs			x					x

Unsuitable / Iinappropriate Aactivities:

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 school or outside school when using school equipment or systems. The school policy restricts usage as follows:

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 (see "User Actions" below).

Social Media - Protecting Professional Identity:

The school provides the following measures to ensure reasonable steps are in place to minimize risk of harm to pupils, 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:

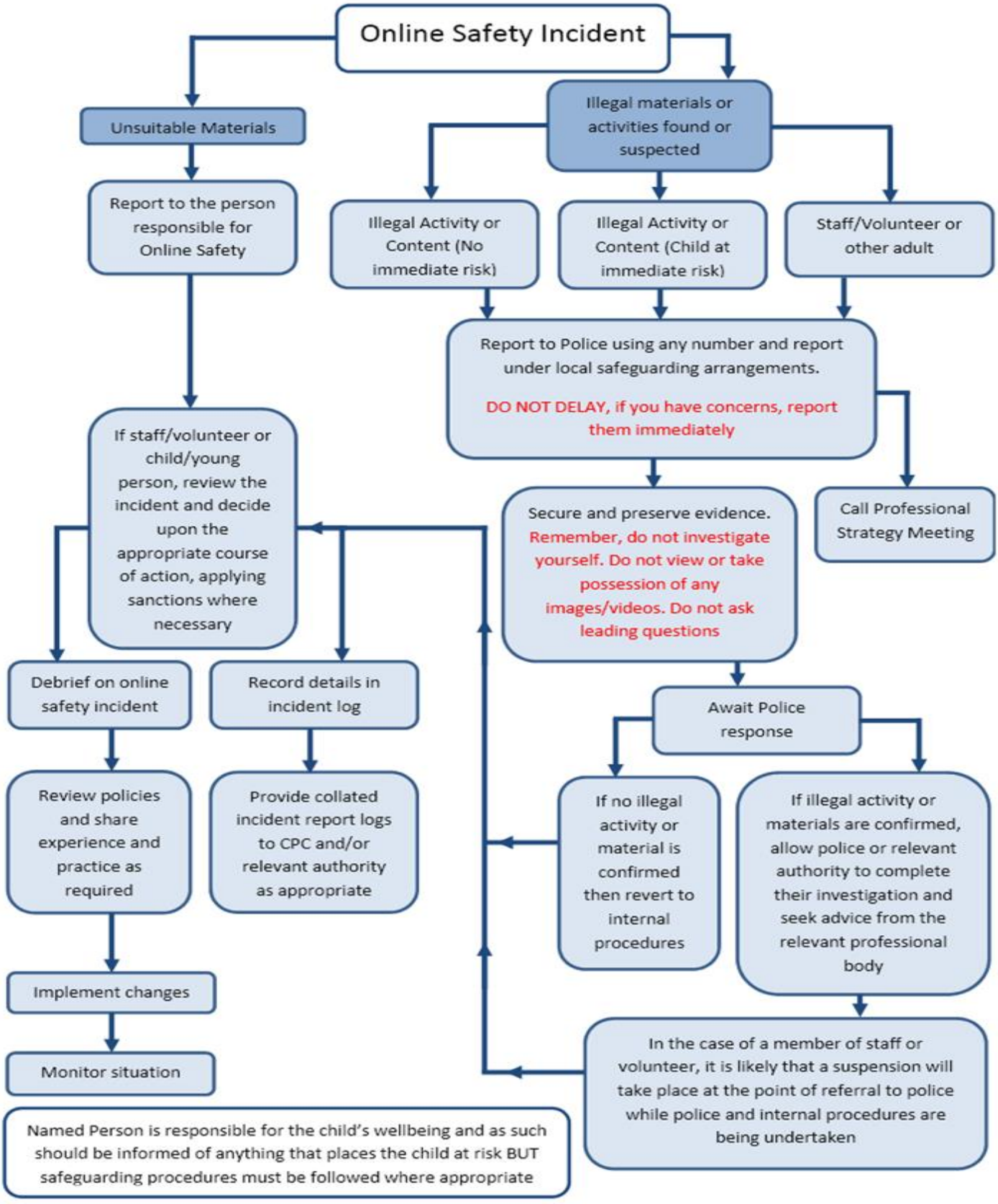
- No reference should be made in social media to students / pupils, parents or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority.
- They are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use.

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 sexual abuse images –The making, production or distribution of indecent images of children					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character)					X
	Ccriminally racist material to stir up religious hatred (or hatred on the grounds of sexual orientation)					X
	pornography					X
	promotion of any kind of discrimination					X
	threatening behaviour, including promotion of physical violence or mental harm					X
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute					X
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)					x	
On-line gaming (non - educational)					x	
On-line gambling					x	
On-line shopping / commerce			x			
File sharing			x			
Use of social media				x		
Use of messaging apps				x		
Use of video broadcasting e.g. YouTube				x		

Illegal Incidents:

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the **right hand side of the Flowchart** below for responding to online safety incidents and report immediately to the Principal.



Internet safety tips that parents should teach their children:

With the advancement in the internet technology, the cybercrime is also increasing. While internet has a plethora of benefits to offer, using it by keeping all the cyber safety and security measures in mind will help you in getting the most out of the internet in a hassle freeway.

According to **Internet crime report**, about two-thirds of the internet users fall victim to cybercrime. There should be a minimum age limit for the kids to use social media. The respective parents should decide as what that age is.

Internet may be a danger zone for uninformed kids:

According to a report by onlineschools.com, about 62 % of the children globally have gone through a negative online experience. Moreover, the kids who use the social networks have more negative experiences than the kids who don't use the social networks.