مدرستنا الثانوية الانجليزية – الفجيرة

OUR OWN ENGLISH HIGH SCHOOL-FUJAIRAH

ONLINE SAFETY POLICY

Online Safety Policy	
Implemented Date	April 2020
Review Date	April 2022
Next Review Date	April 2023

Scope

1 The school is committed to promoting and safeguarding the welfare of all students and an effective online safety is of paramount importance.

1.2 The aims of the school's online safety strategy are threefold:

1.2.1 To protect the whole School community from illegal, inappropriate and harmful content or contact.

1.2.2 To educate the whole School community about their access to and use of technology; and

1.2.3 To establish effective mechanisms to identify, intervene and escalate incidents

where appropriate.

1.3 In considering the scope of the school's online safety strategy, the school will take a wide and purposive approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information including communications technology (collectively referred to in this policy as Technology).

1.4 This policy applies to all members of the school community, including staff, students, parents and visitors, who have access to the School's Technology whether on or off, School premises, or otherwise use Technology in a way which affects the welfare of other students or any member of the school community or where the culture or reputation of the school is put at risk.

1.5 The following policies, procedures and resource materials are also relevant to the

School's online safety practices:

1.5.1 Acceptable Use Policy for Students

1.5.2 E-learning Cyber Safety policy

1.5.3 Digital well-being policy

1.5.4 MOE Student behaviour Management – Distance Learning

1.5.5 Staff Code of Conduct

1.5.6 Computing Policy

1.6 This is a whole School policy and applies to Our Own English High School, Fujairah.

2 Roles and responsibilities

2.1 <u>The Governing Body</u>

2.1.1 The Governing Body has overall responsibility for safeguarding arrangements within the school, including the school's approach to online safety and the use of technology and provide access to appropriate resource required by the IT team and the Principal in safeguarding the online safety of students within the school.

The Governing Body is required to ensure that all those with leadership and management responsibilities at the school actively promote the well-being of students. The adoption of this policy is part of the Governing Body's response to this duty.

2.1.3 The Governing Body will undertake an annual review of the school's safeguarding procedures and their implementation, which will include consideration of the effectiveness of this policy and related policies in meeting the aims set out in paragraph 1.2 above.

2.2 Principal – Online Safety Officer

2.2.1 The Principal has overall executive responsibility for the safety and welfare of members of the school community.

2.2.2 Act and further develop the role of Online Safety Officer.

2.2.3 In addition to leading the online safety group, she should be ensuring that there is effective online safety training and awareness raising.

2.2.4 Delegate and monitor the duties of DSL in terms of reporting incidents, interventions, training to help the aim and objective are achieved, online safety strategies permeating to all levels.

2.2.5 A developing part of their role should be effective delegation of responsibility to others, ensuring that a wide range of relevant staff owns such responsibilities.

2.2.6 The other referred policies are integrated with online safety and child protection, monitor the awareness of online safety reaches all the stakeholders and wider community.

2.2.7 Curriculum planning and delivery gives scope for cross-curricular links to online safety, cyberbullying, child protection and promote digital citizenship.

2.2.8 Other duties:

- Coordinate with the Board of Governors for the safeguarding arrangements with the school.
- Ensure that the appropriate resources are available in safeguarding the online safety of students within the school.
- Designate a senior member of staff to act on her behalf should she be away from the campus.
- The OSL shall identify training needs and conduct adequate training for all members.
- Review the E-safe policies regularly and bring any matters to the attention of the BOG.
- Advise the governing body on all e-safety matters.

- Liaise with the local authority, IT technical support and other government agencies as required.
- Ensure any technical e-safety measures in the school (e.g. Internet filtering software), are fit for purpose through liaison with the local authority and/or ICT Technical Support.

2.3 Senior Leadership Team – Designated Safeguarding Lead

2.3.1 The Designated Safeguarding Leads (DSL) are senior members of staff from the

Senior Leadership Team and the School Counsellor with lead responsibility for safeguarding and child protection. The responsibility of the DSL includes managing safeguarding incidents involving the use of Technology in the same way as other safeguarding matters, in accordance with the School's Safeguarding & Child Protection Policy.

2.3.2 The DSLs will work with the IT Administrator in monitoring Technology uses and practices across the school and assessing whether any improvements can be made to ensure the online safety and well-being of students and provide necessary interventions where required.

2.3.3 The DSLs will regularly monitor the Technology Incident Log maintained by the IT

Manager and the School Counsellor. The school Counsellor also has a prominent role in safeguarding as mentioned in the cyberbullying, child protection and reporting policy.

2.3.4 The DSL will regularly update other members of the SLT on the operation of the

School is safeguarding arrangements, including online safety practices.

2.3.5 Other duties:

- The DSL will regularly update the Principal and other members of the SLT on the operation of the school in safeguarding arrangements, including online safety practices as advised by the Principal.

- The DSL shall ensure the incident logs are maintained by their respective department members.

- The DSL shall ensure that all incidents are appropriately reported and settled. Minutes of all meetings are maintained for future records.

- The DSL shall guide and train teachers on policies, reporting lines, etc. as designated by the Principal.

- The Designated Safeguarding Leads (DSL) are senior members of staff from the Senior Leadership Team. The responsibility of the DSL includes managing safeguarding incidents involving the use of Technology in the same way as other safeguarding matters, in accordance with the School's Safeguarding & Child Protection Policy and instructions, interventions along with the Principal and counsellor where required.

- The DSLs will work with the IT Administrator in monitoring Technology uses and practices across the school and assessing whether any improvements can be made to ensure the online safety and well-being of students and provide necessary interventions where required.

- The DSL will regularly monitor the Technology Incident Log maintained by the IT Administrator Manager and the School Counsellor. The School Counsellor also has a prominent role in safeguarding as mentioned in the cyberbullying, child protection and reporting policy.

- The DSL will regularly update the Principal and other members of the SLT on the operation of the school is safeguarding arrangements, including online safety practices.

- The DSL shall ensure the incident logs are maintained by their respective department members.

- The DSL shall ensure that all incidents are appropriately reported and settled. Minutes of all meetings are maintained for future records.

- The DSL shall guide and train teachers on policies, reporting lines, etc. as designated by the Principal.

- Responsible for monitoring incidents and handling sensitive issues.

- Keep up to date with the latest risks to staff whilst using technology; familiarize themselves with the latest research and available resources for school and home use.

- Review the e-safe policies regularly and bring any matters to the attention of the Principal.

- Update the Principal, governing body on all e-safety matters.

- Engage with staff on e-safety matters at school and/or at home.

- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.

- Ensure any technical e-safety measures in the school (e.g. Internet filtering software), are fit for purpose through liaison with the local authority and/or ICT Technical Support.

- Make themselves aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Principal and responsible governor to decide on what reports may be appropriate for viewing

2.4 Counsellor:

- The School Counsellor with lead responsibility for safeguarding and child protection along with the Online Safety Officer and DSLs.

- All incidents will be reported accordingly to the Principal and DSLs.

- Immediately respond when safety incident occurs

- Saving the evidence

- Assessing the problem

The IT Administrator will provide details on request outlining the current technical

provision and safeguards in place to filter and monitor inappropriate content and to

alert the school to safeguarding issues.

2.3.4 The IT Administrator will report regularly to the SLT on the operation of the school's

Technology. If the IT Administrator has concerns about the functionality, effectiveness,

suitability or use of Technology within the School, s/he will escalate those concerns

promptly to the appropriate members(s) of the School's Senior Leadership Team

(SLT).

2.3.5 The IT Administrator is responsible for maintaining the Technology Incident Log and

bringing any matters of safeguarding concern to the attention of the DSL in

accordance with the School's Child Protection & Safeguarding Policy and Procedures.

2.4 All staff

2.4.1 The school staff have a responsibility to act as a good role model in their use of

Technology and to share their knowledge of the school's policies and of safe practice

with the students.

2.4.2 Staff are expected to adhere, as far as applicable, to each of the policies referenced in paragraph 1.5 above.

2.4.3 Staff have a responsibility to report any concerns about a pupil's welfare and safety in

accordance with this policy and the School's Safeguarding & Child Protection Policy.

2.4.4 Contribute to this policy and digital citizenship to improve the overall online curriculum

of the school.

2.5 Parents

2.5.1 The role of parents in ensuring that students understand how to stay safe when using

Technology is crucial. The school expects parents to promote safe practice when

using Technology and to:

(a) support the school in the implementation of this policy and report any concerns

in line with the school's policies and procedures.

(b) talk to their child / children to understand the ways in which they are using the internet, social media and their mobile devices and promote digital citizenship and responsible behaviour.

(c) encourage their child to speak to someone if they are being bullied or otherwise

are concerned about their own safety or that of another pupil or need support; and

(d) contribute to these policies as when the need arises.

2.5.2 If parents have any concerns or require any information about online safety, they should contact the DSL.

- Determining consequences in accordance with school policies.

- Escalate to the higher authorities.

- Provide the necessary safeguards and support for all pupils involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support

- Inform parents, if appropriate, about the incident and how it is being managed

- If appropriate, advise OSL for referral to external agencies.

2.3 IT Administrator – Online Safety Coordinator

2.3.1 The IT Administrator, together with his team, is responsible for the effective operation of

the school's filtering system so that students and staff are unable to access any

material that poses a safeguarding risk, illegal and inappropriate content and extremist material, while using the school's network.

2.3.2 The IT Administrator as Online Safety Coordinator is responsible for ensuring that:

(a) the School’s Technology infrastructure is secure and, so far as is possible, is not

open to misuse or malicious attack.

(b) the user may only use the School’s Technology if they are properly authenticated

and authorised.

(c) the school has an effective filtering policy in place and that it is applied and

updated on a regular basis.

(d) the risks of students and staff circumventing the safeguards put in place by the

School is minimised.

(e) the use of the School’s Technology is regularly monitored to ensure compliance

with this policy and that any misuse or attempted misuse can be identified and

reported to the appropriate person for investigation; and

(f) monitoring software and systems are kept up to date to allow the ICT team to

monitor the use of email and the internet over the school's network and maintain

logs of such usage.

2.6 Students

The role of students to understand how to stay safe when using Technology is crucial. The school expects students to be aware of safe practice when using Technology.

The safe use of Technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies and tutorial/pastoral activities, teaching students:

(a) about the risks associated with using the Technology and how to protect themselves and their peers from potential risks.

(b) to be critically aware of content they access online and guided to validate accuracy of information.

(c) how to recognise suspicious, bullying, radicalisation and extremist behaviour.

(d) the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect.

(e) the consequences of negative online behaviour; and

(f) how to report cyberbullying and/or incidents that make students feel uncomfortable or under threat and how the school will deal with those who behave inappropriately.

(g) actively participate and contribute to the digital citizenship program.

(h) contribute to this policy via their inputs shared through the Prefects of the Student Council.

<u>3 Education and training</u>

<u>3.1 Students</u>

3.1.1 The safe use of Technology is integral to all School's policies and routines. Students

are educated in an age-appropriate manner about the importance of safe and

responsible use of Technology, including the internet, social media and mobile

electronic devices

3.1.2 Technology is included in the educational programmes followed in the EYFS in the

following ways:

(a) children are guided to make sense of their physical world and their community

through opportunities to explore, observe and find out about people, places,

technology and the environment.

(b) children are enabled to explore and play with a wide range of media and

materials provided with opportunities and encouragement for sharing their

thoughts, ideas and feelings through a variety of activities in art, music,

movement, dance, role-play, and design and technology; and

children are guided to recognise that a range of technology is used in places such

as homes and Schools and encouraged to select and use technology for particular purposes.

3.1.3 The School's Acceptable Use of ICT Policy for Students sets out the school rules about the use of Technology including internet, email, social media and mobile electronic devices, helping students to protect themselves and others when using Technology.

Students are reminded of the importance of this policy on a regular basis.

3.2 Staff

3.2.1 The School provides training on the safe use of Technology to staff so that they are

aware of how to protect students and themselves from the risks of using Technology

and to deal appropriately with incidents involving the use of Technology when they

occur.

3.2.2 Induction training for new staff includes guidance on this policy as well as the Staff

Incident Policy, Code of Conduct, Email & Internet Policy and Professional Use of Social Media Guidelines Policy. Ongoing staff development training includes training on

Technology safety together with specific safeguarding issues including cyberbullying.

3.2.3 Staff also receive data protection guidance on induction and at regular intervals

afterwards.

3.2.4 The frequency, level and focus of all such training will depend on individual roles and

requirements and will be provided as part of the school's overarching approach to

safeguarding.

3.3 Parents

3.3.1 Information is available to parents via the school learning portal. Additionally, we offer the opportunity for parents to attend School based sessions on online safety on an annual basis.

3.3.2 Parents are encouraged to read the Acceptable Use Policy for Students with their

children to ensure that it is fully understood.

4 Access to the School's Technology

4.1 The School provides laptops, internet and intranet access and an email system to all staff as well as other Technology including but not limited to smart board, OHP, etc. Students and staff must comply with the respective Acceptable Use of Technology Policy when using School Technology. All such use is monitored by the IT Administrator and his/her team.

4.2 Students and staff require individual user names and passwords to access the school's

internet and intranet sites and email system which must not be disclosed to any other

person. Any student or member of staff who has a problem with their user names or

passwords must report it to the IT Department immediately.

4.3 No laptop, tablet or other mobile electronic device may be connected to the school network without the consent of the IT Administrator. All devices connected to the school's

network should have current and up-to-date anti-virus software installed and have the latest OS updates applied. The use of any device connected to the school's network will be logged and monitored by the IT Support Department.

4.4 The School has a separate Wi-Fi connection available for use by visitors to the school. A password, which is changed on a regular basis, must be obtained from the IT department in order to use the Wi-Fi. Use of this service will be logged and monitored by the IT Department.

4.5 Use of mobile electronic devices

4.5.1 The School has appropriate filtering and monitoring systems in place to protect students using the Internet (including email text messaging and social media sites) when connected to the school's network.

4.5.2 The School rules about the use of mobile electronic devices are set out in the Acceptable Use of Technology Policy for Students.

4.5.3 The use of mobile electronic devices by staff is covered in the staff Code of Conduct.

Unless otherwise agreed in writing, personal mobile devices including laptop and notebook devices should not be used for School purposes except in an emergency.

4.5.4 The School's policies apply to the use of Technology by staff and students whether on or off School premises and appropriate action will be taken where such use affects the welfare of other students or any member of the school community or where the laws of the UAE, its culture or the reputation of the school is put at risk.

5 Procedures for dealing with incidents of misuse

5.1 Staff, students and parents are required to report incidents of misuse or suspected misuse to the school in accordance with this policy and the school's safeguarding and disciplinary policies and procedures.

5.2 Misuse by students

5.2.1 Anyone as per the incident reporting policy who has any concern about the misuse of Technology by students should report it as per the incident reporting policy, so that it can be dealt with in accordance with the school's behaviour and discipline policies, including the Anti-Bullying Policy where there is an allegation of cyberbullying.

5.2.2 Anyone who has any concern about the welfare and safety of a pupil must report it

immediately in accordance with the School's E-learning Cyber Safety and Anti bullying policy.

5.3 Misuse by staff

5.3.1 Anyone who has any concern about the online safety or misuse of Technology by staff should report it to their line manager who will escalate it to the Principal, so that it can be dealt with in accordance with the staff disciplinary procedures.

5.4 Misuse by any user

Anyone who has a concern about online safety or the misuse of Technology by any other user should report it immediately to the IT Manger or Principal.

5.4.2 The School reserves the right to withdraw access to the school's network by any user

at any time and to report suspected illegal activity to the appropriate government authorities.

Reporting Protocol

Student >Teacher>Supervisor>Counsellor >IT Administrator >Principal

6 Monitoring and review

6.1 All serious incidents involving the use of Technology will be logged centrally in the Technology Incident Log by the IT Administrator.

6.2 The DSL has responsibility for the implementation and review of this policy and will consider the record of incidents involving the use of Technology and the logs of internet activity (including sites visited) as part of the ongoing monitoring of safeguarding procedures, to consider whether existing security and online safety practices within the school is adequate.

Our Own English High School
Fujairah