المدرسة الهندية بالفجيرة
INDIAN SCHOOL FUJAIRAH

Online Safety Policy

2020-21

1. Introduction

1.1 This policy has been developed to ensure that all young people in Indian School Fujairah are working together to safeguard and promote the welfare of children and young people. This policy has been ratified by the Governing Body at the meeting on September 2020.

1.2 E-Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

1.3 This document aims to put into place effective management systems and arrangements which will maximize the educational and social benefit that can be obtained by exploiting the benefits and opportunities by using ICT, whilst minimizing any associated risks. It describes actions that should be put in place to redress any concerns about child welfare and safety as well as how to protect children, young people and staff from risks and infringements.

1.4 The Behavioral Management Committee member or, in their absence, the authorized member of staff for e-safety has the ultimate responsibility for safeguarding and promoting the welfare of pupils in their care.

1.5 The purpose of e-learning in school is to help raise educational standards, promote pupil achievement , support the professional work of staff as well as enhance the school's management information and business administration systems.

1.6 The internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide children and young people with quality access as part of their learning experience.

1.7 A risk assessment will be carried out before children and young people are allowed to use new technology in schools and settings.

2. Ethos

2.1 It is the duty of the school to ensure that every child and young person in its care is safe. The same 'staying safe' outcomes and principles apply equally to the 'virtual' or digital world. This expectation also applies to any voluntary, statutory and community organizations that make use of the school's ICT facilities and digital technologies.

2.2 Safeguarding and promoting the welfare of pupils is embedded into the culture of the school and its everyday practice and procedures.

2.3 All staff have a responsibility to support e-Safe practices in school and all pupils need to understand their Responsibilities in the event of deliberate attempts to breach e-safety protocols.

2.4 E-safety is a partnership concern and is not limited to school premises, school equipment or the school day.

2.5 Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber bullying will dealt with in accordance with the school's Anti-Bullying and Behavior Management Committee.

2.6 Complaints related to child protection will be dealt with in accordance with the school's Behavior Management Committee and The Well Being Team.

3. Roles & Responsibilities

3.1 The Head of Indian School Fujairah will ensure that:

- All staff should be included in E-Safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- A Designated Senior Member of Staff for E-Learning/Safety is identified and receives appropriate on-going training, support and supervision and works closely with the Designated Person for Safeguarding.
- All temporary staff and volunteers are made aware of the school's E- Learning/Safety Policy and arrangements. A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers.

3.2. The Governing Body of the school will ensure that: There is a senior member of the school's leadership team who is designated to take the lead on E-Learning/Safety within the school. Procedures are in place for dealing with breaches of e-safety and security and are in line with Local Authority procedures. All staff and volunteers have access to appropriate ICT training.

3.3 The Designated Senior Member of Staff for E-Learning/Safety will act as the first point of contact with regards to breaches in e-safety and security. Liaise with the Designated Person for Safeguarding as appropriate.

- Ensure that ICT security is maintained.
- Attend appropriate training. Provide support and training for staff and volunteers on E-Safety.
- Ensure that all staff and volunteers have received a copy of the school's Acceptable Use of ICT Resources document.
- Ensure that all staff and volunteers understand and aware of the school's E-Learning/Safety Policy.
- Ensure that the school's ICT systems are regularly reviewed (usually weekly) with regard to security.
- Ensure that the virus protection is regularly reviewed and updated.
- Discuss security strategies with the Local Authority particularly where a wide area network is planned.
- Regularly check files on the school's network.

4. Teaching & Learning

Benefits of internet use for education

4.1 The internet is a part of the statutory curriculum and a necessary tool for staff and children and young people and benefits education by allowing access to world - wide educational resources including art galleries and museum as well as enabling access to specialists in many fields for pupils and staff.

4.2 Access to the internet supports educational and cultural exchanges between students world - wide and enables pupils to participate in cultural, vocational, social and leisure use in libraries, clubs and at home.

4.3 The internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data with the Local Authority.

4.4 The internet improves access to technical support, including remote management of networks, supports

communication with support services, professional associations and colleagues as well as allowing access to, and inclusion in, government initiatives.

4.5 The internet offers opportunities for mentoring pupils and providing peer support for them and their teachers.

4.6 Internet use will be planned to enrich and extend learning activities and access levels will be reviewed to reflect the curriculum requirements and age of the children.

4.7 Children will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

4.8 Children will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information. Children will also be taught that copying material is worth little without an appropriate commentary demonstrating the selectivity used and evaluating the material's significance.

4.9 Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

5. Managing Internet Access

5.1 Developing good practice in internet use as a tool for teaching and learning is essential. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the children.

5.2 Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use.Teachers will guide pupils in on-line activities that will support the learning outcomes planned for the pupil's age and maturity.

5.3 Pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

5.4 If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Coordinator.

5.5 The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

5.6 Pupils will be taught to be critically aware of the materials they read as well as how to validate information before accepting its validity.

6. Managing E-Mail

6.1 Personal e-mail or messaging, chatting on social network between staff and pupils should not take place.

6.2 Staff must use the class website if they need to communicate with pupils about their school work example study leave, course work etc.

6.3 Pupils and staff may only use approved e-mail accounts on the school system and pupils must inform a member of staff immediately if they receive an offensive e-mail. Whole class or group e-mail addresses should be used.

6.4 Pupils must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone.

6.5 Access in school to external personal e-mail accounts may be blocked.

6.6 Pupil e-mail will be restricted.

6.7 E-mail should be authorized before sending to an external organization just as a letter written on school headed note-paper would be.

6.8 Incoming e-mail should be monitored and attachments should not be opened unless the author is known.

7. Managing Website Content

7.1 Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

7.2 Photographs of pupils will not be used.

7.3 The point of contact on the school website will be the school address, school e- mail and telephone number. Staff or pupil's home information will not be published.

7.4 The Section Head or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate.

7.5 The website will comply with the school's guidelines for publications and parents/guardians will be informed of the school policy on image taking and publishing.

7.6 Use of site photographs will be carefully selected.

7.7 The names of pupils will not be used on the website.

7.8 Work will only be used on the website with the permission of the pupil and their parents/guardians

7.9 The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

7.10 Pupils will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimizes or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.

8. Social Networking & Chat Rooms

8.1 Pupils will not access social networking sites.

8.2 Pupils will be taught the importance of personal safety when using social networking sites and chat rooms out of school.

8.3 Pupils will not be allowed to access public or unregulated chat rooms.

8.4 Pupils will only be allowed to use regulated educational chat environments and use will be supervised.

8.5 Newsgroups will be blocked unless an educational need can be demonstrated.

8.6 Pupils will be advised to use nick names and avatars when using social networking sites out of school.

9. Mobile Phones/Devices

9.1 Use of mobile phones/devices for any voice or text communication is not permitted during instructional time.

9.2 Mobile phones/Devices may be used as directed by school personnel. Otherwise, mobile phones/devices must be turned off or muted during instructional time.

9.3 The misuse of permissible electronic devices in a manner distracting devices are deemed distracting to the educational environment.

10. Filtering

10.1 The school will work in partnership with parents/guardians the Local Authority, the Internet Service Provider to ensure systems to protect pupils and staff are reviewed and improved regularly.

10.2 If staff or pupils discover unsuitable sites, the URL and content must be reported to the E-Safety Coordinator.

10.3 Any material the school deems to be unsuitable or illegal will be immediately referred to the Head of the School.

10.4 Regular checks by Senior Staff will ensure that the filtering methods selected are appropriate, effective and reasonable.

10.5 Filtering methods will be selected by the school in conjunction and will be age and curriculum appropriate.

11. Authorising Internet Access

11.1 The school will maintain a current record of all staff and pupils who are allowed access to the school's ICT systems.

11.2 Parents/guardians will be asked to sign and return the school's form stating that they have read and understood the school's 'Acceptable Use' document.

11.3 Staff will supervise access to the internet from the school site for all pupils.

12. Photographic, Video & Audio Technology

12.1 When not in use all video conferencing cameras will be switched off and turned towards the wall.

12.2 Photographic or video technology will not be used in changing rooms or toilets.

12.3 Staff only may use photographic or video technology to support school visits and appropriate curriculum activities.

12.4 Pupils must have permission from a member of staff before making or answering a video conference call, making a video or audio recording in school or on educational activities or taking photographs.

12.5 Video conferencing and webcam use will be appropriately supervised for the pupil's age.

13. Assessing Risks

13.1 Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. The senior leadership team should be aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications.

13.2 In common with other media such as magazines, books and video, some material available through the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to international scale and linked nature of Internet content, it is not always possible to guarantee that unsuitable material may never appear on a school computer. Neither the school nor the Local Authority can accept liability for the material accessed, or any consequences of Internet access.

13.3 Emerging technologies will be examined for educational use and a risk assessment will be carried out before use in school is allowed and methods to identify, assess and minimize risks will be reviewed regularly.

13.4 The Section head will ensure that the E-Safety Policy is implemented and compliance with the policy is monitored.

13.5 Access to any websites involving gambling, games or financial scams is strictly forbidden and will be dealt with accordingly.

14. Introducing The Policy To Pupils

14.1 Rules for Internet access will be posted in all rooms where computers are used.

14.2 Responsible Internet use, covering both school and home use, will be included in the PSHE curriculum.

14.3 Pupils will be instructed in responsible and safe use before being allowed access to the Internet and will be reminded of the rules and risks before any lesson using the Internet.

14.4 Pupils will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately.

15. Maintaining ICT Security

15.1 Personal data sent over the network will be encrypted or otherwise secured.

15.2 Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mails.

15.3 The ICT Manager will ensure that the system has the capacity to deal with increased traffic caused by Internet use.

16. Dealing with Complaints

16.1 Staff, children and young people, parents/guardians must know how and where to report incidents. Concerns related to Safeguarding issues must be dealt with through the school's Safeguarding Policy and Procedures.

16.2 The school's designated person for e-safety will be responsible for dealing with complaints and any complaint concerning staff or pupil misuse of the internet must be reported to the Section Head, Class Teacher immediately.

16.3 Pupils and parents/guardians will be informed of the complaints procedure.

16.4 Parents/guardians and pupils will work in partnership with the school staff to resolve any issues.

16.5 Sanctions for misuse may include any or all of the following:

- Interview / counseling by an appropriate member of staff Informing parents/guardians.
- Removal of internet access for a specified period of time, which may ultimately prevent access to files held on the system, including examination coursework.
- Referral to the police.

17. Parents/Guardians Support

17.1 Parents/guardians will be informed of the school's E Safety Policy which may be accessed on the school website.

17.2 Any issues concerning the internet will be handled sensitively to inform parents/guardians without undue alarm.

17.3 Advice on filtering systems and appropriate educational and leisure activities including responsible use of the Internet will be made available to parents/guardians.

17.4 A partnership approach will be encouraged with parents/guardians and this may include practical sessions as well as suggestions for safe internet use at home.

18. Parents/Guardians Support

18.1 School ICT resources may be increasingly used as part of the extended school agenda.

18.2 Adult users will sign the school's acceptable use policy.

18.3 Parents/guardians of children and young people under 16 years of age will be required to sign the acceptable use policy on behalf of their child.

19. Digital Citizenship

- PARENTS RESPONSIBILITIES

Make sure your child acts responsibly. This includes knowing and understanding the discipline code, Internet Acceptable Use and Safety Policy.

Keep track of your children's online use when they are not in school – including mobile apps, online games and other social media.

Share values with your children and talk with them about what is – and is not – acceptable online behavior.

- STUDENT RESPONSIBILITIES

Follow all school and class rules for using technology

Act responsibly to all both online and face to face.

Collaborate in positive ways that help you learn.

Use technology to support and inclusive school community.

- STAY SAFE

Only use accounts that belong to you

Protect passwords – don't share them with others.

Don't automatically save passwords on school device.

Do not give out personal information online without your parent's permission.

Have permission from a parent before meeting anyone in person that you have met only online.