PO Box 26367
Adliya, Bahrain
Tel/fax: (973) 17728886
info@nadeenschool.com
www.nadeenschool.com
Education License - 7789/74-1/77

Online Safety Policy (E-safety)

| Document ref.	ICT-POL-002
Last Review Date	September 2019
Next Review Date	September 2022
Author	Adam Hegyi
Reviewed by	Liam McCormick
Approved by	Elaine Brennan
Version history	
September 2019	Version 1- Complete rewrite of the previous policy

The purpose of this policy is to:

● Set out the key principles expected of all members of the school community at Nadeen School with respect to the use of IT-based technologies.
● Safeguard and protect the children and staff.
● Assist school staff working with children to work safely and responsibly with the internet and other IT and communication technologies and to monitor their own standards and practices.
● Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use for the whole school community.
● Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies].
● Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
● Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content:

● Exposure to inappropriate content.
● Lifestyle websites promoting harmful behaviours.
● Hate content.
● Content validation: how to check authenticity and accuracy of online content.

Contact:
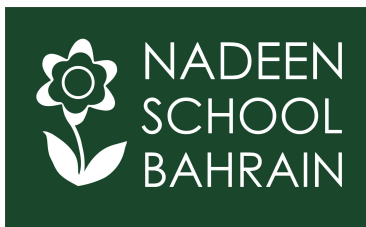
PO Box 26367
Adliya, Bahrain
Tel/fax: (973) 17728886
info@nadeenschool.com
www.nadeenschool.com
Education License - 7789/74-1/77

- Grooming (sexual exploitation, radicalisation etc.).
- Online bullying in all forms.
- Social or commercial identity theft, including passwords.

Conduct:

- Aggressive behaviours (bullying).
- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and well-being (amount of time spent online).
- Copyright (little care or consideration for intellectual property and ownership).

Scope

This policy applies to all members of Nadeen School community (including staff, pupils, volunteers, parents/carers, visitors etc.) who have access to and are users of the Nadeen School IT systems, both in and out of Nadeen School. Computing and the use of digital devices is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Computing and ICT covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of computing within our society as a whole. Currently the apps and software children and young people are using both inside and outside of the classroom include:

- Websites
- Coding
- Educational gaming
- Chromebooks
- iPads
- Android tablets
- Video & Multimedia

Whilst exciting and beneficial all users need to be aware of the range of risks associated with the use of these technologies.

At Nadeen School we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies.
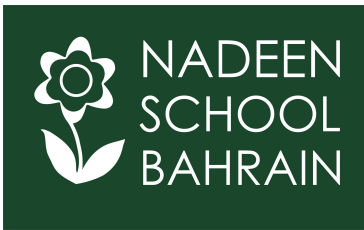
Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of fixed and mobile internet technologies provided by the school. Any visitors using their own devices within school, adhere to the schools Acceptable Use Agreement and this e-safety policy.

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Head and Director have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

This policy, supported by the school's acceptable use agreement, is to protect the interests and safety of the whole school community.

Managing the school e-safety messages

We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used. These messages will be appropriate to the age of the children being taught.

E-safety guidelines will be prominently displayed around the school.

As a school, each year, we also participate in e-safety activities during Safer Internet Day.

E-safety in the Curriculum

The school provides opportunities within a range of curriculum areas to teach about e-safety.

Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-safety curriculum.

The teaching of e-safety focuses on helping children to recognise inappropriate content, conduct, contact and commercialism and helps them learn how to respond or react appropriately.

Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues.

Pupils know how to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member.

Security, Data and Confidentiality

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.
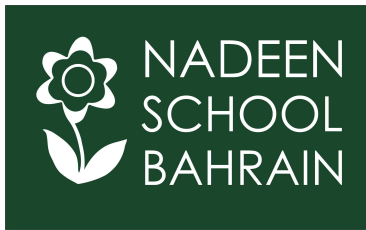
PO Box 26367
Adliya, Bahrain
Tel/fax: (973) 17728886
info@nadeenschool.com
www.nadeenschool.com
Education License - 7789/74-1/77

When accessing, amending and saving any data or information, relating to the school or pupils, school staff follow the guidelines set out in the General Data Protection Regulations 2018.

Managing the Internet

All internet activity within school is monitored and filtered through SafeDNS. Whenever any inappropriate use is detected the incident is followed up in line with the school Acceptable Use Policy.

Students in years 3, 4, 5 and 6 have managed and supervised Internet access through their Chromebooks. Students of other year groups will have supervised access to Internet resources (where reasonable) through the school's digital devices
If Internet research is set for homework, staff will remind students of their e-safety training. Parents are encouraged to support and supervise any further research
 The school uses Hapara software to monitor student's use of technology
Teachers are strongly encouraged to monitor student's web surfing through Hapara on a 3-week block cycle

Infrastructure

Our internet access is provided by Batelco and filtered by SafeDNS.

Staff and students are aware that should they encounter or access anything unsuitable or damaging they must report it immediately to teachers, assistants or the Head of IT.

Mobile Technologies

Personal Mobile devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use during designated times outside of the classroom. These are not to be used at any time whilst children are present.
The school is not responsible for the loss, damage or theft of any personal mobile device.

Managing email

The use of emails within school is an essential means of communication for staff.

Pupils in years 4, 5 and 6 are given school emails that are monitored and restricted to only send and receive emails within the school's domain. Pupils of other year groups currently do not access individual email accounts within school.

Staff must use the school's approved email system for any school business.

Staff must inform (line manager/ Head of IT) if they receive an offensive or inappropriate email.
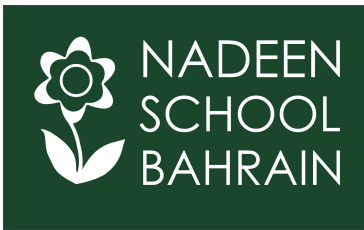
PO Box 26367
Adliya, Bahrain
Tel/fax: (973) 17728886
info@nadeenschool.com
www.nadeenschool.com
Education License - 7789/74-1/77

Social Networking

The school does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day.

The school also strongly discourages children from using age inappropriate social networking outside of school. Should the staff be made aware of incidents or activities on these social networks, which has a direct effect on the children's behaviour or attitudes within school, then the school reserves the right to take action regarding their accounts. This may include discussions with parents, information letters or reporting the child's access to the respective organisations/companies.

Safe Use of Images

Creation of videos and photographs

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

All staff are aware of specific children (they have responsibility for) in school which do or do not have photograph permissions. If they do have permission, staff are aware of which platforms they can be used on.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes field trips. School's own mobile devices must be used in this case.

Publishing pupil's images and work

All parents/guardians will be asked to give permission to use their child's work/photos in publicity materials or on the school website, Instagram account and/or other online platforms.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.

Parents/ carers may withdraw or amend permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa on the school website, Instagram account, or any other school-based publicity materials.
Storage of Images

Images/films of children are stored securely on the school's cloud servers and / or teacher's individual school laptops and other school issued digital devices.
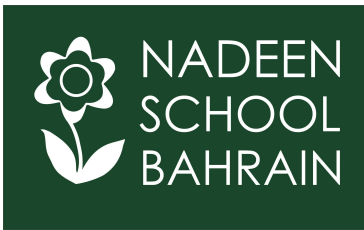
Misuse and Infringements

Complaints

Complaints or concerns relating to e-safety should be made to the line manager or Head of IT.

Inappropriate material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the teacher Head of IT.

Deliberate access to inappropriate materials by any user will lead to the incident being logged and investigated by the Head of IT. Depending on the seriousness of the offence; investigation may be carried out by the Headteacher or School Director. Staff are aware that negligent use or deliberate misconduct could lead to disciplinary action.

How will Cyberbullying be managed?

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone"

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

In the event of cyberbullying:

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include identifying and interviewing possible witnesses, and contacting the parents.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance with the schools anti-bullying and behaviour policy.
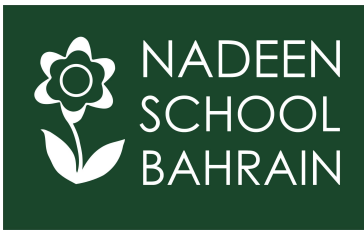
PO Box 26367
Adliya, Bahrain
Tel/fax: (973) 17728886
info@nadeenschool.com
www.nadeenschool.com
Education License - 7789/74-1/77

- Parent/carers of pupils will be informed.
- If the offence takes place off the school site and out of school hours, but is brought to the attention of the school, all children and families involved will be contacted for discussion.

Equal Opportunities

Pupils with additional needs

The school endeavours to deliver a consistent message to parents and pupils with regard to the schools' e-safety rules.

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety.

Internet activities are planned and well-managed for these children and young people.

Reviewing and Monitoring Online Safety

The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school. There is widespread ownership of the policy and it has been approved by the SLT. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.