E-Safety Policy

Introduction

Reach British School is committed to creating 21st Century Learning environments to provide equitable access to technology that will support our students to be self -directed and collaborative learners. The application of digital technologies to teaching and learning at RBS is designed to enrich opportunities for our students learning through in-house resources and effective utilization of wider online platforms. Internet access is an entitlement for students who show a responsible and mature approach to use it. RBS provides students with safe and secure internet access as part of their learning experiences. Our staff plan for the innovative use of technology to provide high quality teaching and learning experiences for their students across the curriculum, while ensuring that online safety is always a priority.

Aims

This policy will outline the steps taken by the school to protect the students from exposure to online harmful materials, communications and behaviors. It also identifies the measures taken by Reach British School to prevent unauthorized access to School Data. In accordance to relevant National Online Safety Website) and local legislation (ADEK Policy 56 Informing Guardians of the School Program, Policy 65 Protection from Dangers of Global Information Network (the Internet)) This policy will;

- Identify the Key roles and responsibilities of the school's community
- Provide clear guidance on the use of school technologies
- Support our staff with online safety
- Support our Students with online safety and effective use of technologies

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

E: info@reachbritishschool.com
T: +971 (2) 582 2030
M: +971 50 852 1801
P.O. Box 12986, Abu Dhabi, U.A.E.

- Regular meetings with the E-Safety Team
- Regular monitoring of e-safety incident logs
- Regular monitoring of filtering / change control logs
- Reporting to relevant Governors / Board / Committee / meeting

Principal and Senior Leaders:

- The Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community.
- The Principal and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e safety allegation being made against a member of staff.
- The Principal and Senior Leaders are responsible for ensuring that the E Safety Team receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Principal 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 those colleagues who take on important monitoring roles.

E-Safety Team: (E-Safety Policy Appendix A - E-Safety Team)

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff
- Liaises with ISP/ADEK initiatives

Network Manager / Technical staff:

- The school's technical infrastructure is secure and not open to malicious attack.
- The school meets required e-safety technical requirements and any ADEK/ other relevant body E-Safety Policy / Guidance that may apply.
- Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- The filtering policy is applied and updated on a regular basis through the MDM and that its implementation is not the sole responsibility of any single person

E: info@reachbritishschool.com
T: +971 (2) 582 2030
M: +971 50 852 1801
P.O. Box 12986, Abu Dhabi, U.A.E.

• 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

• 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

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 through designated courses in the ISP Learning Hub through KnowBe4;

- Security Awareness Training
- Business Conduct Series: Acceptable Use Policy
- Internet Security and You
- Basics of Phishing
- Phishing Attacks on Companies

• They have read, understood and signed the Staff Acceptable Use Agreement (E-Safety Policy Appendix B - Staff Acceptable Use Agreement)

• They report any suspected misuse or problem to the E-safety Team

• All digital communications with students / 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 understand and follow the e-safety and acceptable use policies (Acceptable use agreement Form)

• 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.

• Staff mobile phones should not be used during lesson times . Should a member of staff wish to add a personal device (1 per staff member) A request to IT will be needed, sharing details of device name, MAC Address in order to prioritize the Network to the school's own devices.

E: info@reachbritishschool.com
T: +971 (2) 582 2030
M: +971 50 852 1801
P.O. Box 12986, Abu Dhabi, U.A.E.

Designated Safeguarding Leads

Should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues (Safeguarding and Child Protection Policy) 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
- Cyber-bullying (Cyber Bullying Policy)

Students:

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement (E-Safety Policy Appendix C - Student Acceptable Use Agreement)/ICT Equipment – Secondary.
- 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
- Expected to understand policies on the use of mobile devices and digital cameras.
- They should 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, if related to their membership of the school.

Parents:

Parents play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Parent/Carers Acceptable use of the Internet Agreement (E-Safety Policy Appendix D -Parents and Carers Acceptable Use of the Internet Agreement) The school will take every opportunity to help parents understand these issues through Parent Consultation Days, Coffee Mornings, newsletters,letters, website and information about national / local e-safety campaigns / literature.

Parents will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events

E: info@reachbritishschool.com
T: +971 (2) 582 2030
M: +971 50 852 1801
P.O. Box 12986, Abu Dhabi, U.A.E.

Guidance on the use of School Technologies

The E-Safety Team 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 will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school / academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school academy technical systems.
- Servers,wireless systems & cabling must be securely located and restricted to access.
- Users will have defined access to school / academy technical systems and devices.
- The Network Manager is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations.
- Internet access is filtered for all users EYFS and Primary using Kidrex as a search engine or use of QR codes for specific sites.
- 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 Staff Acceptable Use Agreement (E-Safety Policy Appendix B - Staff Acceptable Use Agreement)
- An appropriate system is in place, IT HELPDesk for users to report any actual / potential technical incident / security breach to the IT Technical Team, 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 workstations are protected by 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.

Support our staff with online safety

The school has an official Facebook, Twitter and Instagram account, managed by the admissions and marketing team. Staff members who have not been authorised to manage, or post to, the account, cannot access, or attempt to access the account. In addition, Entertainment sites are also blocked through the firewall.

The school has guidelines for what can and cannot be posted on its social media accounts

E: info@reachbritishschool.com
T: +971 (2) 582 2030
M: +971 50 852 1801
P.O. Box 12986, Abu Dhabi, U.A.E.

as guided by ISP head office. Those who are authorized to manage the account must ensure they abide by these guidelines at all times.

The school provides each member of staff with an email address. This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email accounts.

- All work-related business should be conducted via school provided email accounts.
- Staff must not share their personal email addresses with parents and students, and must not send any work-related materials using their personal email account.
- Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
- Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.
- Staff must not give their personal phone numbers to parents or students.Staff must use phones provided by the school to conduct all work-related business.

All staff are expected to familiarize themselves and adhere to the following policies/documents relating to online safety:

- RBS Acceptable Use Policy
- RBS Cyber Bullying Policy
- RBS Staff Handbook
- RBS DL Policy
- RBS Social Media Policy
- RBS E- Safety Policy
- RBS Safeguarding Policy
- RBS Behaviour Policy
- RBS Device Responsibility Agreement
- RBS ICT Equipment - Secondary

E: info@reachbritishschool.com
T: +971 (2) 582 2030
M: +971 50 852 1801
P.O. Box 12986, Abu Dhabi, U.A.E.

In addition, at the start of each year all staff carry out mandatory online and face to face safeguarding training that covers the topic of online safety. All staff have access to the national online safety website and complete the annual certificate for online safety which covers the following outcomes:

- Understand key safeguarding legislation and statutory guidance around online safety.
- Recognising how online safety should be implemented in schools and understanding the breadth of online risks and harms to ensure children's safety.
- Identifying how staff should be supporting children around online safety, spotting the danger signs, and responding in a timely and effective manner.
- Understanding how to implement a whole-school approach and developing a culture of online safety to embed policy and process.
- Recognising staff responsibilities around safer use of technology, keeping up to date with online risks and knowing when to seek further advice and support. Staff are expected to always be vigilant and raise any concerns through My Concern, which alerts a Designated Safeguarding Lead who can then ensure timely follow up and appropriate actions.
- Staff have regular weekly updates through whole staff briefings, ongoing CPD opportunities and updates as necessary to ensure best practice.
- Primary Teachers and Specialists follow a Switched On Curriculum that is underpinned by DFE framework Education and covers E-safety within the units of work as well as a bespoke E-safety curriculum that runs in parallel through Assemblies and the PSHE and Citizenship curriculum.
- E-Safety Posters are displayed in classrooms as a reminder of how to stay safe online.
- They have access to a variety of resources to plan high quality online safety lessons and a Digital Learning Coach is available to support any areas of development or guidance required.

Remote access

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site.Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the ICT manager etc. may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with ISP data protection policy.

E: info@reachbritishschool.com
T: +971 (2) 582 2030
M: +971 50 852 1801
P.O. Box 12986, Abu Dhabi, U.A.E.

Support our Students with online safety and effective use of technologies

Provide a systematically filtered service for students Provide supervision and direction in Internet activities Adopt programs that promote safe and ethical behaviours about digital rights and privacy information

At the start of any digital activity staff make reference to the SMART posters to remind students of how to stay safe online.

Set tasks that require students to problem solve through challenging and open questions requiring more than copied and pasted responses from the Internet .

Reinforce the importance of safe, disciplined, ethical, responsible, and respectful use of the Internet in all curriculum areas.

Provide a digital learning curriculum that covers all areas of online safety at an age-appropriate level.

Privacy and Security

Students are taught and encouraged to have good habits when it comes to protecting personal information, including passwords and online safety.

In KS1 they are taught how passwords protect and as they move into KS2 they are taught about the strength of passwords. They are taught why it is important to ask a trusted adult before sharing any personal information with anyone online. Teachers role model best practice. Passwords are not displayed in the classroom and only teachers have access to these should a student forget a password for a school platform or resource through relevant QR codes.

Filtering

The school's Internet access is designed expressly for student use and includes filtering appropriate to the age of the student. Students are taught what is acceptable and what is not and given clear objectives for Internet use.

The school continually monitors, reviews, and updates our firewall system to ensure that students are not able to access inappropriate content or connect through apps and platforms that are not monitored or approved for school use.

Copyright and Ownership

In EYFS and KS1 students learn to acknowledge their own ideas and understand that when they create something using technology it belongs to them. As they progress into KS2 they learn to consider who owns content that they have found online and whether they have the right to re-use it.Moving into KS3 and above, students are made aware of plagiarism and issues relating to work research being undertaken for work.

E: info@reachbritishschool.com
T: +971 (2) 582 2030
M: +971 50 852 1801
P.O. Box 12986, Abu Dhabi, U.A.E.