Al Rabeeh School

E-Safety Policy

Implemented December 2019
Further Reviewed and Update September 2022

<u>Policy Statement</u>
Al Rabeeh School is concerned about the welfare and safety of all its students and attempts to create awareness of how students can feel safe and secure when online and using digital tools.

Monitoring and review
The monitoring and review of this policy is the responsibility of the school leadership team.

<u>Student E-Safety Policy</u>

Ethos

All students have equal rights for care, protection, safety, and security in Al Rabeeh School.

At Al Rabeeh School we believe that it is the right of every and each child to be safe, able to flourish in their learning and protected from abuse. Our prime concern must be the interests and safety of the child. All staff have a duty of care towards all students. Al Rabeeh School (ARS) strives to create an environment in which students feel secure, safe and valued and in which they are listened to and taken seriously.

Staff have a central role in raising awareness and ensuring students understand how to keep themselves safe online as well as be responsible for their own appropriate behaviour online.

This policy provides detailed information to all staff with the necessary guidance for ensuring all students are safe online whilst in our care. It also creates a clear communication with the parents and guardians to inform them how the school will safeguard students.

The school endeavours to work openly with parents/guardians whenever this is possible, however the school does reserve the right to contact the Police directly, without informing parents/guardians if this is deemed in the student's best interests.

Aims

- We aim to safeguard and promote the welfare of all students at the school in compliance with local requirements (ADEK, HAAD)
- We aim to raise awareness for students and parents on how to ensure they stay safe online
- To share the behaviour and code of conduct for online behaviour in school
- To ensure there is a rigorous reporting procedure for any misbehaviour involving use of online platforms and digital equipment related to the school, staff and students.

Keeping Safe Online

The school will:

- Ensure online safety awareness sessions take place in school
- Ensure there are filters to block inappropriate materials from being accessed in school
- To report any instances where students have attempted to search for any inappropriate material in school and report as a safeguarding concern and review school filters

- Share the behaviour code of conduct regarding appropriate use of digital equipment and platforms

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing /moral education / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies, awareness days and pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the pupil Home School Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that 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
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the pupils visit

Education – Parents / Caregivers

Many parents and carers may have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and caregivers through:

- Curriculum activities
- Letters, newsletters, website, infographics
- Parents coffee mornings/ workshops

- Awareness events e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning materials in use of new digital technologies, digital literacy and e-safety
- E-Safety messages targeted towards other relatives as well as parents
- Supporting and networking with community groups (e.g. Early Years Settings, Nannies, youth / sports / voluntary groups) to share their e-safety provision
- Links with outside agencies e.g. Police to give professional advice on how to keep children safe online

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Safeguarding Policy

- The Designated Safeguarding Lead (DSL) and ICT Coordinator (or other nominated person) will receive regular updates through attendance at external training events (e.g. from relevant organisations) and by reviewing guidance documents released by relevant organisations

- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days and reviewed during the termly Safeguarding committee meetings

- The DSL / ICT Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who aremembers of any subcommittee / group involved in technology / e-safety / health and safety / child protection. This maybe offered in a number of ways:

- Attendance at training provided by the external providers recommended by the school

- Participation in school training / information sessions for staff

Technical – infrastructure / equipment, filtering and monitoring

The school 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 named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements

- There will be regular reviews and audits of the safety and security of school academy technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to school 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

- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this

- An appropriate system (My Concern) is in place for users to report any actual or potential technical incident

- 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 up to date virus software

- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Data Protection (followed as guidelines)

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998which states that personal data must be:

- Fairly and lawfully processed

- Processed for limited purposes

- Adequate, relevant and not excessive

- Accurate

- Kept no longer than is necessary

- Processed in accordance with the data subject's rights

- Secure

- Only transferred to others with adequate protection

- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

The school must ensure that:
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed inaccordance with the "Conditions for Processing".

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimizing the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

- Transfer data using encryption and secure password protected devices

Communications

A wide range of rapidly developing communications technologies has the

potential to enhance learning. When using communication technologies, the

school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access)

- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication

- Any digital communication between staff and students or parents / caregivers' (email) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications

- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools a could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimize risk of harm to students, 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 pupils, parents / caregivers 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 ADEK

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.

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 including grooming, online harassment or bullying, sharing of obscene materials, this should be reported immediately to the DSL and recorded on My Concern and, if necessary reported immediately to the police.

Safeguarding During Distance Learning

At Al Rabeeh School, the safeguarding of each and every pupil is vital. The safeguarding procedures followed when learning takes place in Al Rabeeh School is outlined above in this document. The principles within this document are equally as crucial and also need to be applied through Distance Learning.

In the event of a disclosure staff should:

Follow school protocols

- Record the disclosure as soon as possible in the child's own language
- Do not ask any pressing or leading questions
- Do not promise to keep disclosure secret
- Download message from Dojo message / take screenshots
- Record using the School Record Form (Concern form)
- Inform Designated Safeguarding Lead immediately
- Support Designated Safeguarding Lead during investigation
- Remember – a disclosure does not have to be verbalized. It can be something that is seen (bruising, signs of neglect in the background)

When staff create videos, staff must consider the following:

- Environment - videos should be recorded in a suitable location. It is not acceptable to record a video in a bedroom. The background should be neutral, does not have anything contrary to the morals of the UAE (i.e. religious artefacts, artwork or alcohol) in sight and anything that may distract a child from the content of the lesson.
- Clothing - Clothing worn needs to be appropriate and in line with the policy outlined in the *Al Rabeeh School Staff Handbook*
- Content - Ensure the content of the lesson is appropriate and materials are compliant, as outlined in the *ADEK Private Schools Policy and Guidance Manual*
- All videos must be approved by the Head of Year before being posted.

When delivering live lessons, staff must consider all of the above and the following:

- Ensure that you have parental permission and that a parent or appropriate adult is present in the child's home and can be reached quickly at teacher's request

• If a lesson is recorded, the participants are informed at the beginning of the lesson that a recording is taking place
• The child is in an appropriate setting – not their bedrooms.
• Any child who behaves inappropriately during a session is disconnected and parents / HoY are informed as soon as possible.

When approving students work, teachers must consider the following:

• Thoroughly check that the language used is appropriate
• Ensure photographs do not show anything inappropriate and are clear
• Do not share students' work via any platforms other than email (e.g. do not use whatsapp).
• Try to avoid storing photos on your phone – Use Google Drive app to keep photos.
• Do not share students' work with anybody outside of the Al Rabeeh family – with the exclusion of Classroom Monitor for evidence.
• Ensure parent comments on work are appropriate. In the event that they are not, take a screenshot for evidence, report to HoY then delete the comment.

When supporting parents, teachers must consider the following:

• Do not provide any personal details, such as personal email or telephone number
• Do not arrange to meet parents in person
• If parents have a request outside of 'working hours' ensure a response is given by the beginning of the next day at the latest

Distance Learning Student Code of Conduct

All students have been provided with an electronic copy of the *Distance Learning Code of Conduct* and must return the agreements to the school before they can take part in live lessons and / or have access to distance learning platforms.

Access and General Use of ICT: At the start of the academic year, parents will sign a code of conduct agreement. Students must adhere to the following rules when using ICT and internet services:

• Students must use their own email address and login and keep passwords secret
• Students must not attempt to access other peoples files
• Students must not introduce any files or software into the schools computer system (including email, documents, media files, mobile devices etc) unless otherwise agreed by the network manager
• Students must not copy, change, remove or share and programmes or platforms provided by Al Rabeeh School
• Students must not circumvent security measures when accessing school platforms remotely

Use of the Internet: During distance learning, school will only provide and share the details of pre approved websites to support learning. There may also be opportunities for students to research independently. Therefore, we encourage parents to apply the necessary support and parental controls on internet usage and access. When using the internet, students must:

- Not share personal details such as: home address, telephone number, passwords, personal information, photographs of themselves (unless it is sent directly to the class teacher for submission of work), personal details of other students or staff
- Students must not use their school email addresses to sign up for social media websites, create subscriptions or sign up to any websites that may induce spam mail
- Students should not use chatrooms outside of what the school has approved, provided and scheduled
- Students must not arrange to meet anyone they have made contact with online
- Students must not use the internet to cause distress, harass or bully others or incite others to do these things
- Students must not use the internet to bring the school, staff or students into disrepute, or incite others to do this
- Students must not post information about Al Rabeeh School on personal platforms outside of what has been provided and supervised by the school
- Students must respect copyright and understand that submitting work directly from the internet may have implications on assessments and grades
- Students must not change, destroy or delete the data of another student
- Students must tell a member of staff if they feel someone has breached the student/staff code of conduct or if there is something they are concerned about

Sanctions may be given to students following a breach of the student code of conduct.

Email: Each student is provided with an email address and this is used to share notifications, learning materials and access Google Meets for teacher support and live sessions. It is the responsibility of each student (with the support of their parent) to manage their own email account and ensure that they follow the student code of conduct for internet use.

ICT and the Law:

- Most information, photographs etc are copyright and it is important students do not publish this on personal platforms
- Photographs of others should not be shared online unless there is written consent
- Any materials shared by the school should not be reproduced or shared with members outside of the school
- Any queries should be passed on to a member of ARS staff

Distance Learning Behaviour Support

At Al Rabeeh School, during periods of distance learning, we still have high expectations of student behaviour in line with our behaviour policy. Expectations of positive behaviour include:

- Daily attendance for school work
- Professional behaviour during use of live platforms.
- Appropriate messages and correspondence when using online platforms
- Engagement with home learning

Any student who does not adhere to the behaviour expectations and / or demonstrates unacceptable behaviours, as outlined in *Al Rabeeh School's Positive Behaviour Management / Student Conduct Policy (Updated October 2019)* during live lessons, will be removed from the live session and not be allowed to attend live lessons until deemed suitable by the Assistant

Head Teacher. Sanctions will be administered depending on the severity and occurrence of the behaviours, as outlined in the aforementioned policy.

Students who are not engaging with or completing tasks as expected will be contacted by the school administration team.

We are aware that at home, there are different behaviour management strategies amongst families. School will also support students with additional behaviour needs through support for parents e.g. 1:1 online meetings to suggest strategies; meetings with the school counsellor to discuss student behaviour and finding the root cause of any changes in behaviour; online resources and sessions for parents to manage behaviour issues at home. We all also still issue Dojo points and send e-certificates to students for their engagement and behaviour at home in correspondence with the class teacher.

Well Being During Distance Learning

Our School Counsellor is available between 8am and 3.45 daily for any 1:1 support and can be reached via email (noura.dandachli@alrabeeh.sch.ae) or Class Dojo. Online Google Meets can be arranged to discuss support for students and members of the school community. There are also daily online sessions targeted at different groups of people e.g. students, parents etc numerous times per week. We also aim to support students with meeting their social needs and allowing opportunities through teacher supervised Google Meet sessions so they are still able to speak and meet with their peers.

Staff well-being is also a priority as these working hours can become longer and teacher workload can increase. We give the hours of 8:00 until 15:45 for teachers to plan, prepare resources, respond to students' work and parent queries. Work related communication is limited to the hours of 7:30 and 18:00.

Policy Review
This policy will be reviewed annually.

Draft Date:	**2nd September 2022**
Principal Approval:	
Review Date:	**August 2023**

Al Rabeeh School Record Form (Appendix 8)

RECORD OF: Complaint ○ Concern ○ Incident ○ Behaviour ○ Other ○ ……………………………	
Date:	Time:

Present: Student ○ Mother ○ Father ○ Staff Member ○ Visitor ○	
Name of Student:	Class:
Name of Parent:	Contact Number:
Name of Staff Member:	Class/Department:
Name of Visitor:	Contact Number::

Summary:

Action:

Outcome/Follow up:

Al Rabeeh School Body Outline (Appendix 9)

Please use this sheet to show where marks are on the body

Description of Marks