



Title	:	Online Safety Policy
File Name	:	TRAC/ADMIN-OSP/012
Date of Issue	:	1 st April 2024
Next review date	:	31 st March 2025

ONLINE SAFETY POLICY

Introduction

Internet and other digital information communication technologies are excellent tools that pave way to new opportunities in the world of education. Online safety plays an essential part in safeguarding children and young people in the digital age, especially in distance learning platform.

The Governors, staff, students and parents of **The Royal Academy, Ajman** play a vital role in setting an example for the whole school and are central to implementing policy and process. It is imperative that a whole school community approach to online safety is adopted and that all stakeholders are aware of their responsibilities and duties in relation to keeping children safe online. This supports a robust online safety ethos and ensures that the school is providing the best online safety provision they possibly can.

Online safety is an omnipresent topic which requires recurrent regulatory review and places a stringent duty of care on us all. This policy supports school in meeting statutory requirements as per the educational rules and regulations of MoE.

Aim of Online Safety Policy

The Royal Academy, Ajman ensures that :

1. students can safely access new technology and learn how to participate in the digital world without compromising their safety and security .
2. a planned e-safety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited.
3. students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
4. All students and staff understand the importance of password security and the need to log out of accounts.
5. Staff act as good role models in their use of ICT, the Internet and mobile devices
6. It has a clear and understood arrangements for the security, storage and transfer of personal data.
7. to create awareness among the stakeholders on 'the various initiatives of U A E in relation to child protection by incorporating the **Federal Law No: 3 of 2016 (Wadeema's Law)**- **Federal Law No. 3 of 2016** concerning child rights, which states that all children must be provided with appropriate living standards, access to health services, education, equal opportunities in essential services and

facilities without any kind of discrimination, **Federal Law No: 5 of 2012 on combatting cybercrimes** – the article of this law highlights a number of computer and online related activities and how they would be dealt with under the law. It addresses subjects such as IT security, invasion of privacy, malicious and illegal activities including hacking, fraud, improper system use, defamation, threats to state security, terrorism, insult to religions, and many more. etc.

8. It will deal with incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / caregivers of incidents of inappropriate e-safety behaviour that take place out of school.

Links with other policies and practices

The online safety policy links with many other policies, practices and action:

A. Acceptable Use Policy

Introduction

The use of School technology resource is a privilege, not a right. This policy is provided to make all users aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources. If a person violates any of the User Terms and Conditions named in this policy, privileges will be terminated, access to the school's technology resources will be denied, BYOD devices will be denied access to the school's network and Wi-Fi facilities and the appropriate disciplinary action shall be applied. 'The student behavior management policy no: 851 of year 2018' and 'Students' behavior Management in distance learning 2020' shall be applied to student infractions.

Objective

This Acceptable Use Policy is to ensure:

1. That our students will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
2. That school computing systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will ensure that students will have good access to computing to enhance their learning, and we expect the students and parents to agree to be responsible users.

Scope

The policy is applicable to all the students of The Royal Academy School.

Acceptable Use Policy Agreement

I understand that my ward must use school ICT/computing systems in a responsible way, to ensure that there is no risk to their safety or to the safety and security of the Computing systems and other users.

Policy Statement

Student's Role

I understand that:

1. The school will monitor my use of the computing systems and other digital communications on the school equipment.
2. Sharing of passwords, PINs, or other authentic information is strictly prohibited. Everyone is responsible for his/her account(s), including the safeguarding of access to the account(s).
3. The use of ROYAL resources, to access, further or otherwise participate in activity which is inconsistent with the mission of the school is prohibited. This includes, but is not limited to the following: illegal activity, hate speech, violent behavior & bullying, spam, hacking, etc.
4. The school computing systems are for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
5. I need to respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
6. I should not take or distribute images or videos of anyone without their permission. Capturing screenshots of any online class or any member of online class including teachers or students and posting it elsewhere is considered offensive.
7. I should immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online. Will report any kind of safety issues or violations in any form to class teacher.
8. I should not try to open any attachments to emails, unless I know and trust the person/organization who sent the email, due to the risk of the attachment containing viruses or other harmful programs/apps.

Parents Role at home.

1. Keep the computer in a central place, where everyone can see what's on the screen.
2. Stay involved (without stepping on their toes constantly) on what they are doing online –especially if it's got to do with searching and looking for new information etc.
3. Tell them the "No-Can-Go" sites and "No-Can-Play" games rules ahead of time. Check out which sites they want to access, or which games they want to play and tell them if they are acceptable or no-go zones, until they reach a certain specified age.
4. Set time limits. Giving kids unlimited access to online causes unlimited problems for parents. Tell them how many hours they have a week.
5. Explain online habits. Explain strangers often play pretend games and they are not really who they claim to be.
6. Switch Safe Search on as a setting. Most inappropriate content does get filtered by Etisalat or du here in UAE, but there are many slip ups and search results may often have content that's not age appropriate.
7. Remind them that they should not engage in any form of cyberbullying – even as a prank. They should not do anything online that they would be ashamed of doing in real life.

8. Beyond online, watch what content you have on your computer. Often we receive email that is not age appropriate for our children, but we leave that in our mailboxes or desktops. Set the example, clean up.
9. If your children have started to do their homework online, or are gathering information, researching facts etc., explain to them clearly how they should not "copy and paste" (plagiarize) content for their homework, unless they mention sources etc. Their teachers should help them understand this, but you should make it clear that this is not on.
10. Be involved. Be courteous. Be alert. Show on-going interest in what they are playing, reading, doing online. And always remind them that there is life (and a wonderful one) outside that screen.

Staff

1. Educate students on appropriate and acceptable use of devices.
2. Provide guidance to aid students in doing research and help assure student compliance of the acceptable use policy.
3. Monitoring of students' behavior when they are using devices.
4. Report or notify the SLT if any malpractices, issues, or threat found related to the students' use of devices.

Password Policy

The school will be responsible for ensuring that the school network is as safe and secure as possible and that procedures within this policy are implemented. A safe and secure password system is essential and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE). Creating a good password computer is crucial for the safety of the children. It is, therefore, good to set some policies in place while creating passwords for the computers and all online login systems. Some of the possible policies may include:

Length

We recommend a minimum of six (preferably eight) characters in a password for students. The reason for this is because the time one takes to crack a password increases exponentially with its length.

Complexity

Passwords should contain at least one alpha, one numeric and one non-alphanumeric character (a symbol).

Repetition

Change the password on regular intervals and make sure that it is not the same as the previously used passwords. It is recommended that a user does not keep using two passwords over and over again by alternating between them.

Privacy

Do not share passwords with anyone, passwords are to be treated as sensitive and confidential.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, or browsers such as Firefox or Internet Explorer etc.).

User compliance

I understand and will abide by this Acceptable Use Policy. I further understand that should I commit any violation of this policy, my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

B. Child protection policy

Introduction

Child protection refers to the activity which is undertaken to protect children who are suffering or are at risk of suffering significant harm. The Royal Academy, Ajman recognize our moral responsibility to create a safe and supportive environment for all students and to safeguard and promote their welfare. We are fully committed to promoting a safe and welcoming environment for all students, where the students feel respected and valued. All staff are trained to understand the best practices related to protection and safeguarding of all students and appropriate actions to be taken to protect them.

The procedures in this policy apply to all staff, volunteers and governors and are consistent with those of TRAC.

1. The school's responsibility to safeguard and promote the welfare of children is of paramount importance
2. All children, regardless of age, gender, ability, culture, race, language or religion have equal rights to protection
3. Children who are safe and feel safe are better equipped to learn
4. This school is committed to safeguarding and promoting the welfare of children and young people and expects all staff to share this commitment
5. All staff have an equal responsibility to act on any suspicion or disclosure that may suggest a child is at risk of harm at home, in the community or at school
6. If, at any point, there is a risk of immediate serious harm to a child, a referral will be made to relevant statutory body and public services.
7. Students and staff involved in child protection issues will receive appropriate support.
8. This policy will be reviewed at least annually unless an incident, new legislation or guidance suggests the need for an interim review

Aim /Purpose

1. To provide all staff with the necessary information and training to enable them to meet their safeguarding and child protection responsibilities.
2. To ensure consistent good practice across the wider network of TRAC
3. To demonstrate the school's commitment with regard to safeguarding and child protection to students, parents and other partners
4. To establish a safe environment in online, where all students feel safe, cared for, protected and nurtured

Terminology:

1. **Safeguarding** and promoting the welfare of children refers to the process of protecting children from maltreatment, preventing the impairment of health or development, ensuring that children grow up in circumstances consistent with the provision of safe

and effective care and taking action to enable all children to have the best outcomes.

2. **Child protection** refers to the processes undertaken to protect children who have been identified as suffering or being at risk of suffering significant harm.
3. **Staff** refers to all those working for or on behalf of the school, full time or part time, temporary or permanent, in either a paid or voluntary capacity.
4. **Child** includes everyone under the age of 18
5. **Parent** refers to birth parents and other adults who are in a parenting role, for example step-parents, foster carers and adoptive parents

The Royal Academy policy is derived from UAE legislation which includes the following documents:

- **UAE Federal Law No. 3 of 2016 on children's rights (Wadeema's Law)**- concerning child rights, stresses that all children must be provided with appropriate living standards, access to health services, education, equal opportunities in essential services and facilities without any kind of discrimination
- **UAE Department for Health, School Health Guidelines for Private Schools 2011**
- **UAE School Inspection Framework 2016, Section 5, The protection, care, guidance and support of students**
- **'Child Protection Unit' initiative, by the Ministry of Education (MoE)** targeting the students of government and private schools across the UAE aimed at protecting children from all forms of harm, negligence and abuse that they may experience in the surrounding environment at school or at home and maintaining the safety of students from the physical, psychological or educational perspectives.

- In November 2012, the UAE Cabinet approved a draft of "Wadeema's Law" to 'protect' children in the UAE. The law includes creating special units that intervene when children are at risk and stresses that all children have rights regardless of religion and nationality'.
- December 2015 - The Childs Rights Law (previously Wadeema's Law) was passed by the Federal National Council.

We, the faculty and staff, at The Royal Academy, Ajman share the responsibility for keeping our children safe, and are committed to act for the child's best interests.

C. Curriculum Policy/ Integration of E-Safety

Introduction :

The Royal Academy school offers what is typically known as the **CBSE curriculum**, an academic process that is designed and developed by the NCERT, India (National Council of Educational Research and Training, New Delhi).

The school prepares students for the All India Secondary School Examination (at the end of Grade 10) and the All India Senior School Certificate Examination (at the end of Grade 12) conducted by the Central Board of Secondary Education (CBSE), New Delhi, India.

The medium of instruction is English and special emphasis is placed on the teaching of both written and spoken English at all levels. The statutory requirements of Ministry of education UAE will be incorporated- Grade 1 to Grade 9 with compulsory Arabic Studies (as first language for native Arabs), Islamic Studies (Compulsory for all Muslim Students) and UAE National History Curriculum from Grade 1- 9 to meet MOE- UAE equivalency. The proposed curriculum will meet or exceed the minimum CBSE and KHDA standards to ensure an expansive and balanced scholastic experience to our students. Wide range of subjects will be offered at senior secondary levels with flexibility of subject choice.

The Royal Academy has transferred the whole process of Learning and Development to the Virtual world in the present scenario. We use specialized Learning Management Systems with the help of Microsoft Teams to keep a track of learners and educators and in the documentation, reporting, administration of daily learning and assessments. We aim at continual improvement so that our E-Learning is fully competitive with traditional schooling. We also assure that student engagement and peer grouping through collaborative project works because such an atmosphere is far more realistic in terms of preparing students for eventual work life.

Aim and objectives:

The aim of our curriculum is to develop the understanding, knowledge and skills of each student so that they are able to meet the challenges that lie ahead of them in a rapidly changing and competitive world. Through the policy we aim to:

1. Provide a clear rationale based on shared values. The courses, syllabi and activities promote challenge, enjoyment, progression and choice in learning for all students.
2. Provide a curriculum that has breadth and balance across all subjects and within each of its various elements.
3. Plan across the phases of education so as to prepare students well.
4. Provide a curriculum that is regularly reviewed and updated as part of the school's self-evaluation process.
5. Provide cross-curricular themes that are systematically and deliberately planned to ensure that the students' skills across a range of subjects are developed in meaningful and interesting contexts.

The Principal will have over-all responsibility of monitoring the curriculum.

The Kindergarten Section of The Royal Academy, Ajman provides an outstanding start to a child's early learning years. The curriculum is indigenously developed and is based on a well-established international early learning curriculum that is practiced worldwide. Literacy, Numeracy, Discovery and Innovation, Art and Health Education form the core of the syllabus content. There is a wide range of subjects from Primary to Senior Secondary level in each board and there is flexibility of subject choice. The teachers will practice differentiated teaching and learning practice.

At our school, we will provide the opportunity for comprehensive education where both scholastic and Co-scholastic aspects of education are covered like

- Academic
- Work experience
- Physical and Health Education
- Art Education

Along with

- Life Skills
- Attitudes and Values
- Outdoor Activities

This broad-based education will suit the needs of all students. We have devised a policy for curriculum monitoring and support in the school. We firmly believe that educational quality of our school will be directly related to our teaching approaches. We have devised a teaching and learning policy, the purpose of which is to promote rich range of teaching approaches with aims of students making very good progress in their academic studies, learning skills and personal development.

The instructional methods will be based on following principles:

1. **Proper planning** – Through regular meeting of HOD's as part of our curriculum planning
2. **Regular Assessment** for learning- in-class informal continuous comprehensive assessments

3. **Different teaching styles-** Wide range of pedagogic tools and techniques based on the mixed abilities of the class;
4. **Organized online classroom management-** improved quality of classroom relationships
5. **Learning Support Assistants** – high quality of assistance staff and their effective use
6. **Good classroom relationships** – Utilizing teaching methods and resources which interest, motivate students and support the development of their skills
7. **Integration-** Making cross-curricular links while lesson planning;

Regular evaluation and review

The teaching and learning in our school will be a dynamic process with both students and teachers as strong partners. The students in our class-rooms would know

1. How to make progress;
2. What they are achieving through self-assessments;
3. How to learn, including thinking and questioning skills, using methods and resources;
4. The challenges and support available to them;
5. The attitudes needed in the classroom, including respect, interest, responsibility, responding to challenge
6. how to work collaboratively
7. The skills they need to develop, including enquiry, research, analysis, reflection.

Students will be provided a basic frame – work of expectations and guidelines. Teaching through not just directions but activities-based methodology and utilization of educational resources is an important tool to engage student's classrooms. The range of teaching and learning styles used at our School will be extensive. These will include: Explanation, Instruction, Questioning, Observation, Modelling, Investigation, Problem solving, Individual work, Collaborative work , Using ICT, Extended writing, Songs / rhymes, Discussion, Demonstration, Listening, Oral Feedback .During the lesson planning, all aspects of learning is considered which aligns with the objective of the lesson, procedures and activity, assessment, use of resources.

The PHSE Curriculum

As part of the Pastoral Care System there is a programme of PHSE curriculum, which aims to look after the personal, health and social education of all students. It also helps to develop accurate, balanced and relevant knowledge in our students. The programme is structured by including moral education as an integral part of the curriculum.

Aim of the Pastoral Care Programme

1. Develop an individual as a whole person
2. Encourage students through positive affirmation and rewards
3. Raise the standard of performance of each student through self-evaluation.
4. Progress in promoting responsibility, self-esteem and respect.
5. Develop a positive approach to the community in which they reside.
6. To support pupil progress across the curriculum.

Young people clearly face many challenges whilst growing up, and may find at times that they need someone to talk to external to either home or school.

Issues young people may be struggling with include: Bullying, Academic pressure, Low mood, Anxiety, Exam stress, Adolescent stage, Over Influence of the electronic media

Counselling is a process which offers support and guidance when things feel particularly difficult. The counsellor will provide a safe and confidential place for a young person to explore thoughts and feelings which perhaps are overwhelming and upsetting, in a drive to enable change

D. Password protection policy

Overview

Password protection is a security process that protects information accessible via computers that needs to be protected from certain users. Password protection allows only those with an authorized password to gain access to certain information. The policy is applicable to all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that belongs to WPS(Wi-Fi Protected Setup), resides at any WPS location, has access to the WPS network, or stores any WPS information.

Scope of Password Security Policy

The school will be responsible for ensuring that the school network is safe and secure as possible and that procedures within this policy are implemented. A safe and secure password system is applied to all school technical systems, including networks, devices,

email and Virtual Learning Environment (VLE). To ensure the online safety of the stakeholders, a strong password system is mentioned.

Policy Procedures

The Royal Academy, Ajman Password Policy includes: -

1) Password Creation / Sharing Policy:-

1. All the password will be created and issued by the IT Admin as per the request of staff members.
2. The school official parent communication platform which has been activated when the child enrolled in campus and the IT Admin is responsible for future communications
3. The VLE passwords are created by the ICT teacher as per the instructions getting by the IT Admin.
4. While constructing the password for VLE, an option strictly maintained to change the first sign in.
5. All our school network connected devices such as Laptops, LED Panels, Printers etc. were set up with the strong password.
6. All the Users are trained about password protection and the password policy that implemented.
7. IT systems are configured to prevent password reuse.
8. Passwords on their expiry shall cease to function
9. All user accounts are protected by strong passwords and that the strength of the passwords meets the security requirements of the system as follows.
10. We are ensuring the safe and secure password sharing system to circulate all the stakeholders which has been created by the IT Admin/ In charges.
11. While sharing the password, we are instructing the stakeholders to reset their password when they first sign in.
12. The VLE passwords are shared to the stakeholders through the any of our official communication system.
13. All the system-level passwords are changed every 180 days and shared individually through any of the official communication channel.

Instruction for creating the password

1. Should contain 8 characters
2. Should contain alpha numeric characters
3. Should include special character (e.g., ~, !, @, #, \$, ^, (,), _ , +, =, -, ?,)
4. Contain at least one number (e.g., 0-9)
5. Should contain upper- & lower-case characters (Aa - Zz)
6. Should not include personal data
7. Should not repeat any characters more than twice
8. Should not contain a dictionary word in any language, slang, dialect, jargon, etc

II) Reset Password / Deleting Password :-

1. IT Admin is the overall in charge to manage and implement all the password related issues.
2. We implemented the account lockout strategy in VLE. This shall be based on a risk analysis of the system to trying with more than two wrong attempts the system will automatically locked and the user have to contact the IT Admin resetting the password
3. All passwords will meet the following criteria:
4. All system-level passwords (e.g., root, admin, application administration accounts) must be changed at least every 180 days.
5. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 30 days. - Passwords must NOT be inserted into email messages or other forms of electronic communication.
6. All user-level and system-level passwords must conform to the guidelines described below
7. If any of the stakeholders are resigning from our organization, we will make sure that to delete all the accounts related to the concern person will be removed from our domain and ensure our data security.

III) Password Maintenance Policy:-

1. Don't reveal your password over the phone to ANYONE
2. Don't reveal your password to any supervisor
3. Don't reveal your password in an email message
4. Don't talk about your password in front of others
5. Don't hint at the format of your password (e.g., "my family name")
6. Don't reveal your password on questionnaires or security forms
7. Don't share your password with family members
8. Don't reveal your password to your friends
9. Don't write passwords down and store them anywhere.
10. Don't store passwords in a file on ANY computer system
11. Don't use the "Remember Password" feature or the "Remember Me" on any application that contains sensitive data.
12. Don't use the same password for more than one account.

E. Cyber bullying policy etc.

Introduction:

The Royal Academy, Ajman recognize that technology plays an important and positive role in everyone's lives, both educationally and socially. It is committed to helping all members of the school community to understand both the benefits and the risks, and to equip children with the knowledge and skills to be able to use technology safely and responsibly. Research into cyberbullying indicates that it is a feature of many young people's lives. Cyberbullying, like all other forms of bullying, should be taken very seriously.

Aim:

Aim of this policy is to ensure that:

1. we safeguard the pupils in the real and virtual world.
2. students, staff and parents are educated to understand what cyberbullying is and what its consequences can be.
3. knowledge, policies and procedures are in place to prevent incidents of cyberbullying in school or within the school community.
4. we have effective measures to deal effectively with cases of cyberbullying.
5. we monitor the effectiveness of prevention measures.

Definition for Cyber-bullying :

Cyber-bullying is "the use of information and communications technology, particularly mobile phones and the internet, deliberately to upset someone else." It is an aggressive, intentional act carried out by a group or an individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself

By cyber-bullying, we mean bullying by electronic media:

1. Bullying by texts or messages or calls on mobile phones
2. The use of mobile phone cameras to cause distress, fear or humiliation
3. Posting threatening, abusive, or humiliating material on websites, to include blogs, personal websites, social networking sites
4. Using e-mail to message others
5. Hijacking/cloning e-mail accounts

Policy procedure:

The Royal Academy educates students both in the proper use of technology and about the serious consequences of cyberbullying. With the help of proper curriculum links and computing lessons we continue to inform students in these fast-changing areas. All students and teachers must sign the Acceptable Use of Technology Agreement. All members of the school community are aware they have to bring to the attention of the online safety group any example of cyber-bullying or harassment or misuse of technology that they know about or suspect.

Whilst education and guidance remain at the heart of what we do, The Royal Academy will take action against those who take part in cyber-bullying in line with the guidelines in the Anti-Bullying policy. Students are encouraged to report any suspicions of cyberbullying and have access to the concerned and proper guidance is offered to victims of cyberbullying including emotional support and reassurance.

Roles and Responsibilities**a) Students:**

If you believe you or someone is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, or a member of staff on your safety network.

1. Do not answer abusive messages but save them and report them

2. Do not delete anything until it has been shown to your parents/carers or a member of staff at school (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyber-bullying)
3. Do not give out personal details or contact information without the permission of a parent/guardian (personal data)
4. Be careful who you allow to become a friend online and think about what information you want them to see.
5. Protect your password. Do not share it with anyone else and change it regularly.
6. Always log off from the computer when you have finished or if you leave the computer for any reason.
7. Always put the privacy filters on to the sites you use. If you are not sure how to do this, ask a teacher or your parents.
8. Never reply to abusive emails
9. Never reply to someone you do not know.

b) Students:

It is vital that parents/carers and The Royal Academy work together to ensure that all students are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying.

1. Parents/carers must play their role and take responsibility for monitoring their child's online life.
2. Parents/carers can help by making sure their child understands The Royal Academy policy and, above all, how seriously we take incidents of cyber-bullying.
3. Parents/carers should also explain to their children legal issues relating to cyber-bullying.
4. If parents/carers believe their child is the victim of cyber-bullying, they should save the offending material (if need be by saving the offensive text on their computer or on their child's mobile phone) and make sure they have all relevant information before deleting anything.
5. Parents/carers should contact the school as soon as possible.
6. Parents/carers should attend the school's training on online safety delivered by the ICT support.

c) Staff:

All staff have a responsibility to prevent misuse of equipment and cyberbullying

1. Ask the students to get up on-screen the material in question.
2. Ask the students to save the material.
3. If possible, Print of the offending material straight away.
4. If possible and with the student's agreement a screen capture image may be able to be sent to the staff's school email account .
5. Inform a member of the Senior Leadership team and pass them the information that you have.

F. E-Communication Policy

Introduction

The Royal Academy E- communication policy functions as a guideline for its staff and students , instructing them on how to appropriately use the electronic mode of communication .

Policy Guidelines:

1. **Official Text message:** The Royal Academy Ajman send official SMS text message through its own centre id "TRAC AJMAN" which is officially registered in ETISALAT.
2. **Internal Communication:** Internal extension are provided through IP phone, in the campus.
3. **Email:** All the staff are provided with official mailid, which has to be used for any mode of official communication.
4. **Orison Communication:** Parents have a registered mobile number with school Orison software for communication.
5. **Telephone Contact :**Any general enquiry related to school should be through the following contact persons only- Reception, Admissions Officer, Parent Relation Executive
6. **Auto Bcc policy:** To Keep transparency, the immediate line manager is put for Auto Bcc by the stakeholder.

Monitoring and Review of the Policies

The Royal Academy Ajman reviews this policy and practices quarterly, in accordance with any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.

Approved By
Principal

