أكاديمية بلومنجتون، عجمان

The Bloomington Academy, Ajman

Learn. Share. Grow.

ONLINE SAFETY POLICY

INTRODUCTION

At ***Bloomington Academy, Ajman*** we understand the responsibility to educate our pupils in e-Safety issues; teaching them the appropriate behaviors and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

All children, whatever their needs, will have access to a range of up to date technologies in both the suite and classrooms. ICT is a life skill and should not be taught in isolation.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognize the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children are using both inside and outside of the classroom include

- Websites
- Learning Platforms and Virtual Learning Environments (VLE)
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Downloading from the internet
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality.

All users need to be aware of the range of risks associated with the use of these Internet technologies.

Aim of Online Safety Policy

The Bloomington Academy, Ajman ensures that:

- students can safely access new technology and learn how to participate in the digital world without compromising their safety and security.
- a planned e-safety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited.
- students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- All students and staff understand the importance of password security and the need to log out of accounts.
- Staff act as good role models in their use of ICT, the Internet and mobile devices
- It has a clear and understood arrangements for the security, storage and transfer of personal data.
- 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 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.

- It will deal with incidents within this policy and associated behavior and anti-bullying policies and will, where known, inform parents / caregivers of incidents of inappropriate e-safety behavior 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

We in ***The Bloomington Academy, Ajman*** are pleased to be able to offer our students, staff and guests' access to computer technology, including access to the internet, Microsoft Teams 365 platform. We are dedicated to access and support of appropriate technology which unlocks our potential and connects us locally and globally. We envision a learning environment where technology is a part of us, not apart from us.

We believe that the tremendous value of technology and the information technology network as an educational resource far outweighs the potential risks. We will leverage existing and emerging technology as a means to learn and thrive in the 21st Century and prepare our students for success toward their goals in the competitive global, electronic age. We feel that access to the tools and resources of a world-wide network and understanding when and how these tools are appropriately and effectively used are imperative in each student's education.

The school's information technology resources, including email and Internet access, are provided for educational purposes. If you have any doubt about whether a contemplated activity is acceptable, consult with your immediate teacher, supervisor, Principal to help decide if a use is appropriate. Adherence to the following policy is necessary for continued access to the school's technological resources:

Users must respect and protect the privacy of others by:

1. Using only assigned accounts.
2. Only viewing, using, or copying passwords, data, or networks to which they are authorized.
3. Refraining from distributing private information about others or themselves.

Users must respect and protect the integrity, availability, and security of all electronic resources by:

1. Observing all school Internet filters and posted network security practices.
2. Reporting security risks or violations to a teacher or network administrator.
3. Not destroying or damaging data, networks, or other resources that do not belong to them, without clear permission of the owner.
4. Conserving, protecting, and sharing these resources with other users.
5. Notifying a staff member or administrator of computer or network malfunctions.

Users must respect and protect the intellectual property of others by:

1. Following copyright laws (not making illegal copies of music, games, or movies).
2. Citing sources when using others' work (not plagiarizing).

Users must respect and practice the principles of community by:

1. Communicating only in ways that are kind and respectful.
2. Reporting threatening or discomforting materials to a teacher or administrator.
3. Not intentionally accessing, transmitting, copying, or creating material that violates the school's code of conduct or honor code (such as messages/content that are pornographic, threatening, rude, discriminatory, or meant to harass).
4. Not intentionally accessing, transmitting, copying, or creating material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works).
5. Not using the resources to further other acts that are criminal or violate the school's code of conduct or honor code.
6. Avoiding spam, chain letters, or other mass unsolicited mailings.
7. Refraining from buying, selling, advertising, or otherwise conducting business, unless approved as a school project.

Users may, if in accord with the policy above:

1. Design and post web pages and other material from school resources.
2. Communicate electronically via tools such as email, chat, text, or videoconferencing.
3. Install or download software, if also in conformity with laws and licenses.
4. Use the resources for any educational purpose during school hours.

Consequences for Violation

Violations of these rules may result in disciplinary action, including the loss of a user's privileges to use the school's information technology resources. Further discipline may be imposed in accordance with the school's code of conduct and honor code up to and including suspension or expulsion depending on the degree and severity of the violation.

Supervision and Monitoring

The use of school owned information technology resources is secure, but not private. School and network administrators and their authorized employees monitor the use of information technology resources to help ensure that uses are secure and in conformity with this policy. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement.

The school reserves the right to determine which uses constitute acceptable use and to limit access to such uses. The school also reserves the right to limit the time of access and use.

ICT Acceptable Use Policy for pupils:

Agreement / e-Safety Rules

- I will take care when using the school IT equipment and use it properly.
- I will only share my user name and password with trusted adults.
- I will tell an adult if I see anything that upsets me.
- I will make sure that when I blog, I am responsible, polite and sensible.
- I will use a safe name and not my real name on the internet.
- I know I am only allowed to go on the internet if my teacher has given me permission.
- I will only take a photograph or video of someone if they say it is alright.
- Any messages I send will be polite.
- I will not deliberately write anything which upsets other people.
- I understand that the school may talk to my parent or carer if they are worried about my use of school IT equipment.
- I understand that if I do not follow these rules, I may not be allowed to use the school computer or internet for a while, even if it was done outside school.

We have discussed this and ………………………………………………. (child's name)
agrees to follow the e-Safety rules and to support the safe use of ICT at

The Bloomington Academy, Ajman.

Parent / Carer (Name) …………………………………………………….

Parent / Carer (Signature) ……………………………………………………………

Class ………………………………………………. Date………………………

Acceptable Use of ICT Agreement

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with a member of SLT.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorized by the Head or Governing Body. USB sticks containing data must be encrypted. These are supplied by school.
- I will not use or install any hardware or software without permission from the ICT technician.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken with school devices, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be

distributed outside the school network without the permission of the parent/ carer, member of staff or Head of section.

- I understand I cannot use my mobile phone to take photos of children
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request by the Head of section.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature ……..……………….……………… Date …………………..

Full Name ……………………………………………………………………..

Job title: ……………………………………………………………………..

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:

The health, safety and well – being of all our children are of paramount importance to all the adult who work in our school. Our children have the right to protection, regardless of age, gender, race, culture or disability. They have a right to be safe in our school.

Protecting children is everyone's responsibility at our school and this includes reporting any act committed by a parent, guardian or any other person., to a child enrolled in the school which in neglect, physical or emotional injury or sexual harm.

All staffs have a duty and will report any suspected or disclosed issues of child protection to the Designated Child Protection Officer (DCPO) / Child Protection

Team. If the threat is immediate or on – going it will be reported to the appropriate local safeguarding authority as set in place by the UAE.

Policy Statement:

The safeguarding of children and young people from harm is the highest priority here at ***The Bloomington Academy***. Our students have a right to feel safe and protected from significant physical and emotional harm both inside and outside of school. An effective whole- school child protection policy is implemented in our school to promote the welfare of our students; this policy is a crucial part of promoting it is designed to inform our staff regarding the signs of child abuse and to equip them with the knowledge on what to do in the event of suspected abuse. This policy defines abuse, outlined signs of abuse and explains the procedures for investigating and reporting suspected cases. It also shows our school's commitment to the development of good practices and sound procedures. The policy ensures that child protection concerns, referrals and monitory may be handled sensitively, professionally and in ways which support the needs of the child.

Aims and Objectives:

This policy ensures that all staff in our school can follow the necessary procedure with regard to a child protection:

- To raise awareness and identify responsibility in reporting possible cases of abuse;
- To ensure effective communication between all staff when dealing with child protection issues;
- To inform all parties of the correct procedures to use in the case of a child protection issues.

Types of child abuse

Physical abuse

This may involve hitting, shaking, throwing, poisoning, burning or scalding, drowning, suffocating or otherwise causing any physical harm to a child. Physical harm may also be caused when a parent or career fabricates the symptoms of, or deliberately induces illness in a child. It is necessary for the teacher to identify this.

Emotional Abuse

Includes persistent emotional maltreatment and/ or verbal abuse towards a child, causing adverse effect on the emotional development of a child. It may involve conveying to children they are worthless, unloved, and inadequate or valued only in so far as they meet the needs of another person. It may cause the child to feel frightened, in danger, or to be exploited or corrupted.

Sexual Abuse

Involving forcing or enticing a child to take part in sexual activities, whether or not they are aware of what is happening. It may involve physical contact, penetrating or non – penetrating acts and also includes children in looking at, or encouraging children to behave in sexual inappropriate ways.

Neglect

This is the persistent failure to meet a child's basic physical and / or psychological needs which is likely to result in serious impairment to their health and development. It may involve a parent or career failing to provide adequate harm or danger, or allow access to medical care or treatment. It may also include the neglect of, or unresponsiveness to, a child's basic emotional needs.

<u>When to be concerned</u>

Staff should be concerned if a student:

- Has any injury which is not typical of the bumps and scrapes normally associated with the child activities
- Regularly has unexplained injuries
- Frequently has injuries even apparently reasonable explanations are given
- Offers confused or conflicting explanations about how injuries were sustained
- Exhibits significant changes in behavior, performance or attitude
- Indulges in sexual behavior which is unusually explicit and/ or inappropriate to his or her age
- Disclose an experience in which he or she may have been harmed

If a student discloses that he or she has been harmed in some way, the member of the staff should:

- Listen to what is being said without displaying shock or disbelief.
- Accept what is being said
- Allow the child to talk freely
- Reassures the child but do not make promises that it might be impossible to keep.
- Reassures the pupil that what has happened is not their fault.
- Stress that it was the right thing to tell
- Listen rather than ask direct questions.
- Ask open questions rather than leading questions
- Not criticize the perpetrator.
- Explain what has to be done next and who has to be told.

General principles:

- All staff should be alert to the sign of abuse and neglect and know to whom they should report concern or suspicions.
- The SDC team members are the first point of contact for staff and parents where a concern is identified.
- The school ensures that any full, part – time or volunteer staffs and parents are security checked prior to employment/engagement. This is a whole school requirement and includes all ancillary staff as well as academic teaching staff.

Operational Procedure:

When a child report abuses the teacher / staff will inform the SDC team members immediately. If there are reasonable causes to believe that some abuse is occurring and the child is unable to reveal it, it must soon be brought into notification. The Student Development Officer and SDC team members will take initial steps to gather information regarding the reported incident. At this stage she/ they will:

- Interview staff members as necessary and document information relative to the case.
- Consult with school personnel to review the child's history in the school.
- The Student Development Officer and SDC team members will then form a school-based response team to address the report. The response team may include the school doctors, nurse, teacher and other individuals as the Student Development Center (SDC) ascertains. In all cases, follow up activities will be conducted in a manner that ensures that information is documented factually and that strict confidentiality is maintained.

Based on acquired information, a plan of action will be developed to assist the child and family. Action that may take place are:

- Discussion between the child and the SDC in order to gain more information.
- In – class observations of child by SDC.
- Meeting with the child's family to present the school's concerns.
- Referral of the student and family to external professional counseling if necessary.
- Consultation with local authorities.

Subsequent to a substantiated case of child abuse or neglect, the following actions may take place:

- The SDC will maintain contact with the child and family to provide support and guidance as appropriate.
- The SDC will provide the child's teacher with ongoing support, and provide strategies for the teacher to use.
- The SDC will maintain contact with outside therapists, in order to update the therapist about the progress of the child in school, and to keep the school informed about the progress of the therapy.
- The School Principal refers the case to local authorities for further action.

Specific responsibilities of:

School Doctor/Nurse

- The Doctor or Nurse may require conducting an examination if there are physical injuries and write an initial report about child physical and emotional condition.
- Child abuse can lead deep emotional scars and School Doctor or Nurse should recognize these and help develop a rehabilitation plan in liaison with the SDC team members and other appropriate staff members.
- In some cases, the child may have to take medication as a result of the abuse, the School Doctor or Nurse should ensure that all standards and procedures for administrating medications in the school setting are met.

Security Staff

- The security staff undertake to be vigilant and adhere to the procedures governing the access and detailed record – keeping.
- Provision of a visitor's pass to be worn for ease of identification and monitoring of visitor's to the school.

Child Protection Officers

The following persons are to be contacted for all child protection issues at THE BLOOMINGTON ACADEMY, Ajman**.**

1. Teacher
2. Counsellor / Coordinators / Supervisors
3. School Doctor/ School Nurse
4. Senior Leaders Team (Principal, /Head Of Sections) T

The Bloomington 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 Bloomington 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

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety.

- We provide opportunities within the ICT curriculum areas to teach about e-safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the curriculum.

- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling, and activities as part of the ICT curriculum.
- Pupils are aware of the impact of online bullying through PSHE and are taught how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies (cyber bullying)
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum
- Pupils are taught about the risks inherent in using social media, particularly if they are contacted by people, they do not know.

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 Bloomington Academy, Ajman **Password** Policy includes:

a. Password Creation / Sharing Policy

- All the password will be created and issued by the IT Admin as per the request of staff members.
- 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

- The VLE passwords are created by the ICT teacher as per the instructions getting by the IT Admin.
- While constructing the password for VLE, an option strictly maintained to change the first sign in.
- All our school network connected devices such as Laptops, LED Panels, Printers etc. were set up with the strong password.
- All the Users are trained about password protection and the password policy that implemented.
- IT systems are configured to prevent password reuse.
- Passwords on their expiry shall cease to function
- All user accounts are protected by strong passwords and that the strength of the passwords meets the security requirements of the system as follows.
- 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.
- While sharing the password, we are instructing the stakeholders to reset their password when they first sign in.
- The VLE passwords are shared to the stakeholders through the any of our official communication system.
- All the system-level passwords are changed every 180 days and shared individually through any of the official communication channel.

b. Instruction for creating the password

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

c. Reset Password / Deleting Password: -

- IT Admin is the overall in charge to manage and implement all the password related issues.
- 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 Admit resetting the password
- All passwords will meet the following criteria:
- All system-level passwords (e.g., root, admin, application administration accounts) must be changed at least every 180 days.
- 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.
- All user-level and system-level passwords must conform to the guidelines described below
- 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.

d. Password Maintenance Policy:-

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

E. Cyber bullying policy

Introduction:

The Bloomington 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:
- we safeguard the pupils in the real and virtual world.
- students, staff and parents are educated to understand what cyberbullying is and what its consequences can be.
- knowledge, policies and procedures are in place to prevent incidents of cyberbullying in school or within the school community.
- we have effective measures to deal effectively with cases of cyberbullying.
- 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:

- Bullying by texts or messages or calls on mobile phones
- The use of mobile phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, or humiliating material on websites, to include blogs, personal websites, social networking sites
- Using e-mail to message others

- Hijacking/cloning e-mail accounts

Policy procedure:

The Bloomington 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.
- Do not answer abusive messages but save them and report them
- 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)
- Do not give out personal details or contact information without the permission of a parent/guardian (personal data)
- Be careful who you allow to become a friend online and think about what information you want them to see.
- Protect your password. Do not share it with anyone else and change it regularly.

- Always log off from the computer when you have finished or if you leave the computer for any reason.
- 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.
- Never reply to abusive emails
- Never reply to someone you do not know.

b. parent/carers

- It is vital that parents/carers and ***The Bloomington 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.
- Parents/carers must play their role and take responsibility for monitoring their child's online life.
- 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.
- Parents/carers should also explain to their children legal issues relating to cyber-bullying.
- 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.
- Parents/carers should contact the school as soon as possible.
- 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
- Ask the students to get up on-screen the material in question.
- Ask the students to save the material.
- If possible, Print of the offending material straight away.
- 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.
- Inform a member of the Senior Leadership team and pass them the information that you have.

F. E-Communication Policy

Introduction

The Bloomington 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:

- **Official Text message**: The Royal Academy Ajman send official SMS text message through its own center id “TBAC AJMAN” which is officially registered in ETISALAT.
- **Internal Communication**: Internal extension are provided through IP phone, in the campus.
- **Email**: All the staff are provided with official mail id, which has to be used for any mode of official communication.
- **Orison Communication**: Parents have a registered mobile number with school Orison software for communication.
- **Telephone Contact:** Any general enquiry related to school should be through the following contact persons only- Reception, Admissions Officer, Parent Relation Executive
- **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 *Bloomington 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.

Implementation Date: 1st April 2020
Reviewed on : 25th October 2020

Review Date: As require
Monitored by : Principal/Senior Leadership Team