TBAC/POLICY/ESAFE/001/2023-2024 **Date: 01.08.2023**

E-Safety Policy

Updated By	Reviewed on	Monitoring Cycle
Online Esafety Leader	August 2023	1 Year

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governing Body on:	September 2023
The implementation of this e-safety policy will be monitored by the:	SLT
Monitoring will take place at regular intervals:	Annually
The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Annually
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	2024
Should serious e-safety incidents take place, the following external persons/agencies should be informed:	Ms. Hussaina Sheriff (Principal)

The school will monitor the impact of the policy using: (delete / add as relevant)

- Logs of reported incidents
- Surveys of reported incidents:
  - Students
  - Parents / Caregivers Staff

Scope of the Policy

This policy applies to all members of the school (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school. At TBAC we are committed safeguarding our students through prevention, protection and support. We believe that everyone in the school community has the right to learn and to teach in a supportive and caring environment without the fear of being bullied. We are committed to helping all members of the school community to benefit from information and communication technology, while understanding its risks, and to equip children with the knowledge and skills to be able to use it safely and responsibly. The school recognises that any bullying incident should be treated as a child protection concern when there is reasonable cause to believe that a child is suffering or likely to suffer significant harm.

This E-Safety policy enables our school to create a safe e-learning environment that policy supports school in meeting statutory requirements as per the educational rules and regulations of MOE and to create awareness among the stakeholders on 'the various initiatives of UAE in relation to child protection. 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. covered by the published Behaviour Policy of MOE. The school will deal with such 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.

Roles and Responsibilities

Principal and Senior Leaders:

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

Online Safety Leader

- Leads the e-safety committee
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provides training and advice for staff
- Liaises with the MOE / relevant body
- Liaises with school technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Attends relevant meeting and reports regularly to Senior Leadership Team.

Online Safety Coordinators

- Make sure they have an up-to-date awareness of e-safety matters and of the current school / academy e-safety policy and practices.
- Work closely with the online safety leader in leading the committee and all roles and responsibilities.
- Follow up on the plans for the year and ensure that they are being carried out systematically.
- Advice the online safety leader of any deviations from plans or any breaches that need attention for the leader and the group.
- Guide the Student Online Safety Group in their activities.
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned 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

Child Protection Officer (School Counsellor)

- Take the lead along with online safety leader in ensuring in child protection.
- Immediately respond or step in when an online child safety incident occurs and work with the online safety leader, parents and students as required to address the same.
- Ensure that the evidence of intervention is documented.
- If appropriate, advise Online Safety Leader and school leadership for referral to external agencies.
- Be a part of the development, implementation and reviewing of the child protection policies of the school.
- Actively participate in the development of training modules for stakeholders on child protection, online behaviours and anti-bullying.
- Obtain training on handling various child protection and e-safety issues and stay updated on the same.

Digital Ambassadors (Student Representatives)

- Actively participate and contribute to the digital citizenship program.
- Take the lead in the planning of events and activities for creating student awareness about e-safety.
- Report any trends or incidents that would have come to their purview to the online safety leader.
- Come up with ideas for improving student responsibility when it comes to the use of digital technology and discuss the same with the group to convert it into concrete plan of action.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

Parents / Caregivers:

- Encourage the implementation e-safety norms prescribed by the school for the home environment.
- Work with the school in the promotion of digital citizenship and responsible behaviour.
- Alert the school in case of any issues that comes to the attention of the parent rep.
- Work with the school for the implementation of policies that pertain to students and parents.

Training the TBAC Community

Training Online Safety Group

It is essential for the school leadership as well as members of the Online Safety Group to be equipped. For this the school ensures that they obtain relevant training from outside accredited organizations as well as experts in the field on the same. The school management shall also see to it that the leadership and the group attend webinars and conferences to keep themselves updates and bring about improvements in TBAC e-safety initiative.

Training Parents and Students.

Training students as well as parents 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 recognize and avoid e-safety risks and build their resilience.

- Induction program for parents and students on e-safety at the beginning of the academic year.
- Periodic posters, tips and articles sent to parents and students (age appropriate) on digital safety.
- Classroom activities and events that involve students so that they learn about e-safety hands on.
- Minimum of three student awareness programs in a year.
- Minimum of two parental awareness programs in a year.
- Incorporating e-safety in other subjects where chapters enable the same.
- Ensure that students are given due classes on digital citizenship.
- Distribution of updated student handbooks to both parents and students at the beginning of every academic year.
- The important helpline numbers provided on the website.
- Oath taken by students at the beginning of every year on e-safety.
- Acceptable usage agreement is signed by every parent on behalf of their wards when they join the school.
- Parents are explained the relevance of the Media Release Consent Form and they sign the same at the beginning of the academic year.
- Reminders sent to parents to read up and understand e-safety guidelines posted on website.
- Updates on policies and guidelines communicated to parents and students when such updates occur.
- School newsletter and posters which highlights e-safety as well.
- Student council active involvement in educating their peers about e-safety.

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.
- 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 Acceptable Use Agreements.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings.
- The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

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 / academy meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school academy technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school / academy technical systems and devices.
- The online safety coordinators are responsible for ensuring that software licenses 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/academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (trainee teachers, supply teachers, visitors) onto the school systems.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / caregivers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

- Student's full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website.
- Students' work can only be published with the permission of the pupil and parents or carers.

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 in accordance with the "Conditions for Processing".
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.

Communications

When using communication technologies, the school considers the following as good practice:

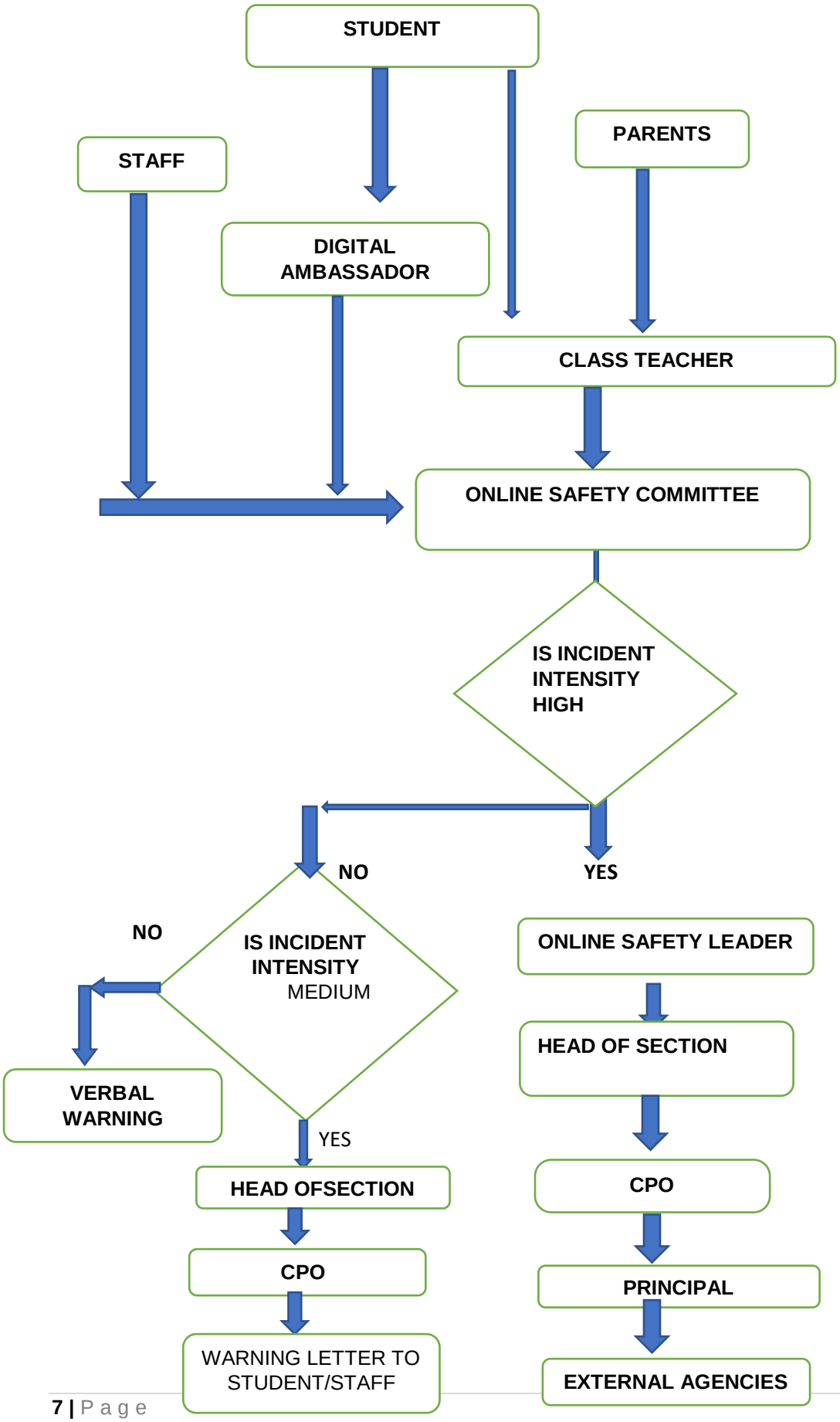
- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems.
- Users must immediately report to the online safety coordinators – in accordance with the school / academy 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.
- Whole class / group email addresses may be used at KG, while student pupils at Grade 1 to 11 will be provided with individual school email addresses for educational use.
- 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.

E safety incidents reporting mechanism

Based on the severity of the issue the reporting and handling mechanism is carried out as mentioned in the online incident reporting flow chart. The below table mentions the action that will be taken in case of such incidents in brief:

Intensity	Staff	Action plan	Student	Action plan
Low	Reporting to Online safety team	Verbal warning	Reporting to Class Teacher/Digital Ambassador	Verbal Warning
Medium	Reporting to Head of Section	Warning letter/memo with suspension.	Report to Online Safety Team	Report to parents and warning letter to students.
High	Reporting to Senior Leadership and Management	Immediate termination from job and reporting to external agencies.	Report to Senior Leadership Team.	Report to parents and external agencies.

Incident Reporting Protocol



Emergency Contact Details for Reporting

School stakeholders can always approach the school directly or seek help from the following when there is an incident.

School Contact Details

Front Desk: 067478780

School Mobile Number: 0569940429

Mail ids: esafe@thebloomingtonacademy.com

Guidelines of MOE on Online Safety

The school ensures to follow all the guidelines laid by MOE and incorporate into the system for the well-being and security of the whole school community. The sanctions set forth by the Ministry is also adhered to. TBAC is aware of MOE's child protection unit specially designed to implement the mechanisms and measures of child protection in educational institutions as stipulated in the Federal Law No. 3 for 2016 and its executive regulations. Ministry of Education (MOE) has launched a 'Child Protection Unit' initiative for the benefit of students of government and private schools across the UAE. The initiative is aimed at protecting children from all forms of harm, negligence, and abuse which they may experience at school or home and maintaining their safety with regard to their physical, psychological and educational aspects.