Approved by: Principal	Date:	01/10/2024

Last reviewed on:	Date:	01/10/2024

Next review due by:		Date:	01/10/2025

Revision History

#	Description of Changes	Rev. No	Date of Issue
1	First Issue	00	01/10/2024

This policy applies to all staff, including senior managers and the board of trustees, paid staff, shadow teachers, volunteers and sessional workers, agency staff, students or anyone working on behalf of the Sheikh Khalifa Bin Zayed Arab Pakistan School (SKBZAPS).

Policy Statement

SKBZAPS is dedicated to ensuring a safe and supportive digital environment for all students from Kindergarten through Grade 12. This comprehensive digital policy integrates guidelines on acceptable use of IT, e-safety, and cyberbullying, in alignment with ADEK and UAE Ministry of Education requirements, as well as best international practices.

Purpose

The purpose of this policy is to:

- Provide a safe digital environment for all students.
- Educate students, staff, and parents on responsible digital behaviour.
- Prevent and address cyberbullying.
- Protect the school community from inappropriate content and cyber threats.

Legal Framework

This policy is based on the following:

- ADEK Policy and Guidance Manual
- UAE Federal Law No. 3 of 2016 on Child Rights (Wadeema's Law)
- UAE Federal Law No. 5 of 2012 on Combating Cybercrimes
- UAE Federal Law No. 12 of 2016 amending Federal Law No. 5 of 2012

- International best practices in digital safety and cyberbullying prevention

Roles and Responsibilities

- **Governing Body**:
  - o Ensure the policy is implemented and reviewed annually.
  - o Allocate resources for digital safety initiatives.
- **Principal**:
  - o Oversee the implementation of the policy.
  - o Ensure staff are trained and aware of their responsibilities.
  - o Act as the main point of contact for digital safety issues.
- **E-Safety Coordinator (Vice Principal)**:
  - o **Role**:
    - ▪ Coordinate e-safety initiatives within the school.
    - ▪ Act as the main point of contact for e-safety concerns.
  - o **Responsibilities**:
    - ▪ Develop and implement e-safety policies and procedures.
    - ▪ Maintain detailed records of e-safety concerns and actions.
    - ▪ Ensure staff receive regular training on e-safety.
    - ▪ Liaise with ADEK and other relevant authorities.
- **IT Officer**:
  - o Ensure adequate safeguards are in place to filter and monitor inappropriate content.
  - o Maintain and update virus protection software.
  - o Report any e-safety concerns to the E-Safety Coordinator.
- **Teachers and Support Staff**:
  - o Promote and model safe and responsible use of technology.
  - o Report any concerns or incidents of cyberbullying to the E-Safety Coordinator.
  - o Integrate e-safety education into the curriculum.
- **Parents and Guardians**:
  - o Support the school's digital policies and monitor their child's use of technology at home.
  - o Report any concerns about their child's digital safety to the school.
- **Students**:

o Follow the school's digital policies and guidelines.

o Report any inappropriate content or cyberbullying to a teacher or the E-Safety Coordinator.

Acceptable Use of IT

- **General Use**:
  - o Students must use school IT resources responsibly and for educational purposes only.
  - o Personal use of IT resources is prohibited without explicit permission.
  - o The use of personal devices is allowed only for pre-arranged educational activities and with permission from a teacher.

- **Internet and Email**:
  - o Students must not access inappropriate content or engage in illegal activities.
  - o Personal information, such as addresses and phone numbers, must not be shared online.
  - o School email accounts must be used responsibly and for school-related communication only.

- **Security**:
  - o Students must not download or install unauthorized software.
  - o All digital work must be virus-scanned before use on school computers.

E-Safety and Cyberbullying

- **Education and Awareness**:
  - o E-safety education is integrated into the curriculum to teach students about online safety, privacy, and responsible digital behaviour.
  - o Regular workshops for parents to help them support their child's online safety.

- **Reporting and Response**:
  - o All incidents of cyberbullying or inappropriate online behaviour must be reported to the E-Safety Coordinator.
  - o The E-Safety Coordinator will assess the situation and take appropriate action, which may include contacting parents or relevant authorities.

- **Support for Victims**:

  o The school provides counselling and support services for students affected by cyberbullying.

  o Actions are taken to ensure the safety and well-being of the victim.

Confidentiality and Data Protection

- All information related to digital safety concerns is confidential.
- Information is shared only with relevant authorities and personnel involved in the case.
- Records of digital safety cases are securely stored and access is restricted to authorized personnel.

Monitoring and Review

- The policy is reviewed annually to ensure it remains effective and up-to-date with legal requirements and best practices.
- The E-Safety Coordinator monitors the implementation of the policy and reports any issues to the governing body.

Templates for Compliance

- **Student E-Safety Agreement**:
  - o Students must read and sign the E-Safety Agreement, acknowledging their understanding and compliance with the school's digital policies.
- **Parent E-Safety Agreement**:
  - o Parents must read and sign the E-Safety Agreement, acknowledging their support for the school's digital policies and their role in monitoring their child's online behaviour.

Contacts

- **Vice Principal**: [Name and Contact Information]
- **IT Officer**: [Name and Contact Information]

Appendix 1

Student E-Safety Agreement

I agree to:

- Use ICT systems in school responsibly and for school purposes only.
- Keep my passwords secure and not share them with anyone.
- Report any inappropriate content or cyberbullying to a teacher or the E-Safety Coordinator.
- Follow the school's rules on the use of the internet and digital devices.

Student Name:

_____

Student Signature:

_____

Date:

_____

Class:

Appendix 2

Parent E-Safety Agreement

I agree to:

- Support the school's digital policies and monitor my child's use of technology at home.
- Attend school workshops on e-safety to better understand how to support my child's online safety.
- Report any concerns about my child's digital safety to the school.

Parent/Guardian Name:

Parent/Guardian Signature:

Date:

Child's Name:

_____

Class:

_____