ICT and E-Safety Policy

This policy sets out the aims, principles and strategies for the delivery of information and Communication Technology (ICT). This is a working document due to the rapid and continual advances and developments in the fast-moving world of technology.
As well as being an important curriculum requirement the ability to use ICT effectively is a vital skill in modern society.

Through the use of ICT across the curriculum, KNES aims to help students gain knowledge, skills and understanding about the nature of information, be confident in using a range of technology and have the skills and understanding to exploit potential. The use of ICT is promoted within all subjects.

This Policy is in place to ensure the safety and wellbeing of all students at Kuwait National English School. The **Safeguarding and Child Welfare** elements are at the foundation of everything we do at KNES.

The policy will be under annual review or updated as needed.

We strive to achieve our aims by:

➢ **Ensuring children and young people are using and interacting in ICT in a way that they are Safeguarded against abuse of any sort and are exposed to positive influences.**
➢ Using ICT where possible to enhance students learning in all areas of curriculum
➢ Introduce students to a wide range of ICT applications and ICT tools, such as word processing, databases, graphics and use of the interactive white boards.
➢ Helping students acquire the skills to use appropriate ICT tools effectively for learning and leisure.

- Equipping students with knowledge of the uses, effects and limitations of ICT enabling them to evaluate its benefits and impact on society.
- Meeting the British National Curriculum requirements as fully as possible and helping all students to achieve the highest standard of achievement
- Using ICT to develop partnership beyond the school through the use of the internet and email
- Celebrating success in the use of ICT

ICT resources will include the following hardware and software

- Interactive whiteboards
- Access to computers and laptops
- Printers
- A range of software for word-processing, presentations, databases, spreadsheets, clipart, desktop publishing, multimedia presentation (film, animation and music) art and photography, age appropriate applications (apps), email.
- Variety of information and communication technology games, gadgets and tools used in everyday life.
- Pictures, photographs, books, posters, video clips for reference, teaching about the history of ICT, inventions, inventors and for creative inspiration.

Mobile Phones; Mobile phones are banned from all students in school unless a special exemption is provided by the Head of Department.

Filtering
The school will work in partnership with parents / guardians, Ministry of Education and our Internet Service Provider to ensure systems to protect pupils and staff are reviewed and improved regularly.

If staff or students discover unsuitable sites, the URL (address) and content must be reported to the Head of Department immediately.

Regular checks by Senior Staff will ensure that the filtering methods selected are appropriate, effective and reasonable.

Authorizing Internet Access

➢ All staff must read and sign the School's "Staff Code of Conduct.

➢ The school will maintain a current record of all staff and students who are allowed access to the school's ICT systems.

➢ Parents / Guardians will be asked to sign and return a copy of the Schools acceptable use of ICT before being allowed to access the ICT resources.

Photographic, Video and Audio Technology

➢ It is not appropriate to use photographic or video technology in changing rooms or toilets.

➢ Staff may use photographic or video technology to record and support School trips, special events, assessment evidence and other appropriate curriculum activities.

➢ Audio and video files may not be downloaded without prior permission of the network manager.

Responsibilities

The Head of School is responsible for:

➢ Ensuring staff access to ICT

➢ Arranging in-service support

➢ Meeting curriculum requirements

➢ Health and safety policy and practice

The ICT Coordinator is responsible for

➢ Advice concerning appropriate software to meet the needs of the policy in conjunction with the Ministry of Education expectations.

➢ Purchasing and organizing ICT resources

➢ Identifying what ICT support is needed by individual staff

➢ Ensuring the consistent implementation of the ICT policy

➢ Ensuring continuity between year groups

➢ Ensuring progression of learning for all students in ICT

➢ Reviewing ICT policy and making recommendations to the SMT

➢ Reviewing the ICT subject development plan

The Class teacher is responsible for:

➢ Record-Keeping and assessment of students

➢ Ensuring equal access for all students

➢ Developing and applying the ICT curriculum across other curriculum areas.

Assessing Risks

Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and develop good practice. The senior leadership team are aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications.

In common with other media such as magazines, books and video, some material available through the internet is unsuitable for students. The school will continue to take all reasonable precautions to ensure that users access only appropriate material. However, due to the International scale and linked nature of internet content, it is not always possible to guarantee that unsuitable material may never appear on a School computer.

The school cannot accept liability for the material accessed or any consequences of Internet Access.

Emerging technologies will be examined for education use and risk assessment will be carried out before use in the school is allowed and methods to identify, assess and minimize risks will be reviewed by the ICT Coordinator.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence.

The School Director will ensure that the E-safety policy is implemented and compliance with the policy is monitored.

Access to any websites involving gambling, games or financial scams is strictly forbidden and will be deal with accordingly.

Introducing Policy to Students

➢ Rules for internet access will be posted in all rooms where computers are used.

➢ Responsible internet use, covering both school and home use, will be included in the PSHE curriculum

➢ Students will be instructed in responsible and safe use before being allowed access to the internet and will be reminded of the rules and risks before any lesson using the internet.

➢ Students will be informed that Internet use will be closely monitored and the misuse will be dealt with appropriately.

Consulting Staff

➢ It is essential that teachers and learning support staff are confident about using the internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies. This is best done in the staff members Department meeting.

- All staff are governed by the terms of the School's Staff Code of Conduct and will be provided with a copy of the School's Internet Policy and its importance explained.
- All new staff will be given a copy of the policy during their induction and part of the introduction to Safeguarding training.
- Staff development in the safe and responsible use of the internet will be provided as required.
- Staff will be aware that internet use will be monitored and traced to the original user. Discretion and professional conduct is essential.
- Senior managers will supervise staff who operate the monitoring procedures (middle Managers / ICT coordinator)

Maintaining ICT Security

- Personal data sent over the network will be encrypted or otherwise secure.
- Unapproved system utilities and executable files will not be allowed in students' work areas or attached to emails.
- The ICT teacher, in liaison with the SMT, will ensure that the system has the capacity to deal with increased traffic caused by internet use.

Dealing with Complaints

Staff, parents / guardians, children and young people must know how and where to report incidents. Concerns related to Safeguarding issues must be dealt with through the School's Safeguarding Policy and Procedures.

The Schools Designated Safeguarding Lead as well as the Head of Department will be responsible for dealing with complaints and any complaint concerning staff or student misuse of the internet must be reported to the School Director immediately.
Students and parents / guardians will be informed of the complaints procedure. Parents / guardians and students will work in partnership with School staff to resolve any issues.

There may be occasions when the school has to contact the police or Child Protection Services. If appropriate, early contact should be made to discuss strategies and preserve possible evidence.

Sanctions for misuse may include any or all of the following:

➢ Interview / counseling by an appropriate member of staff

➢ Informing parents / guardians

➢ Removal of internet access for a specified period of time, which may ultimately prevent access to files held on the system=, including examination coursework.

➢ Referral to police.

Parental Support

➢ Parents / guardians will be informed of the school's Internet Policy which may be accessed on the School Website and in communication provided in the Parent / Pupil handbook.

➢ Any issues concerning the internet will be handled sensitively to inform parents / guardians without undue alarm.

➢ Advice on filtering systems and appropriate educational and leisure activities including responsible use of the internet will be made available to parents / guardians

General Use of Computers

➢ The use of School computers will be permitted only for purposes directed by the school.

➢ Users are not permitted to access and amend another user's work without permission.

➢ All PC's connected to the internet will be protected by anti-virus software which wil be kept up to date to check for the latest viruses.

➢ No files should be brought from home and loaded on the school system without permission of the ICT Manager.

> ➢ The school reserves the right to look at any files on their systems including text, graphics and emails.
> ➢ The school reserves the right to deny access to its computer systems.

Health and Safety

The school is aware of the Health and Safety issues involved in student's use of ICT. T