IBS INTERNATIONAL BRITISH SCHOOL
Aspire. Achieve. Advance

**ASPIRE ACHIEVE ADVANCE**

# ICT Safety Policy

## Introduction

e-Safety encompasses internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils and staff about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-Safety policy should operate in conjunction with other policies including those for Behaviour Management Policy, cyber-bullying, portable device acceptable use, Internet acceptable use - staff and pupil.

## 1. Rationale:

This policy is designed to meet the school's obligations to maintain a safe learning environment for staff and students. The overall goal is to maximize the educational benefits of communication technologies while minimizing the risks.
This ICT Safety Policy applies to all employees of the school and to all students. It also applies to teacher and other professional trainees assigned to the school from time to time.

### End to End e-Safety

e-Safety depends on effective practice at a number of levels:

- Responsible IT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-Safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering systems

## 2. Aims:

Use of computers, the internet and other communication technologies at IBS is to be limited to educational usage appropriate in the school environment including professional development.

The communication technologies are available to staff and students under certain conditions, as outlined in the computer/cyber safety use agreements. The school will provide training for the staff and students with respect to the appropriate use of these technologies.

This policy, its procedures and the User Agreements refer to the appropriate use of computers, fax, phone, internet, scanners, copiers, email, mobile phones, digital cameras, video cameras, web cams, DVD's and video within the school.

Appropriate cyber safety measures will be put in place and enforced by the school management team and the HOD ICT with the support of ICT staff. In order to ensure the safety of the school learning environment, action will be taken if these safety regulations are breached by students or staff.

The school staff will follow the agreed guidelines to prevent any use of the internet for purposes other than education. When using these technologies, the school will endeavour to minimize and where possible, stop students or staff using these to:

- Have contact with or possession of objectionable and questionable material. This includes pornography, violence, weapons, drugs, defacing of individuals, seditious material, breaches of Kuwait/International law and obscene written materials.
- Have contact with questionable persons .
- Pass on inappropriate materials.
- Violate privacy and access rights.
- Illegally use copyright material.
- Illegally download software.
- Use technologies to harass or bully others.

## 3. Guidelines:

**a.** The Principal and management team will be responsible for the support of the ICT technician who will be responsible for the maintenance of an ICT safety program in the school.

**b.** The necessary procedures will be put into place by the school to address ICT safety issues where the internet and other communication technologies are used inappropriately or illegally by staff or students.

**c.** Training for staff can be made available by management and the ICT staff.

**d.** Students will be supervised by staff while using school ICT facilities. The degree and type of that supervision may vary, dependent on the type of technology concerned, where the equipment is physically situated and whether or not the student is able to access the internet.

**e.** The school will provide an effective electronic filtering security system as well as setting all preferences to 'safe' modes. If deemed necessary, auditing of the school computer system will include all aspects of its use including personal network storage folders, use of internet via IP address and school based e-mail accounts.

**f.** The ICT technician and members of the senior management team will undertake this audit.

**g.** The principal maintains the right to check communication technology-related work or data of staff or students at any time and to carry out a comprehensive investigation of any breaches of the school's ICT safety policies. Such breaches will be taken seriously and be dealt with through the school's disciplinary and support systems. In such incidents, there will be special attention paid to the need for specific procedures as regards the gathering of evidence. If illegal material or activities are suspected, the matter will be reported to the police.

**h.** The school will consult with the wider school community and provide opportunities to learn about cyber safety issue e.g. through newsletters and parent information sessions.

**i.** Educational material on cyber safety will be provided by management to staff and students, and to parents/caregivers. As well, additional safety education will be delivered, where relevant, through teaching programs

**j.** **Writing and reviewing the e-safety policy:**

  **i.** The e-Safety Policy is part of the School Development Plan and relates to other policies including those for IT and for child protection.

  **ii.** The school's e-Safety Coordinator is also the It technician with an input from the ICT teacher and the Head of Humanities/ICT. They work in close co-operation with the Head of Primary and the Head of Secondary

  **iii.** e-Safety issues are included in the Child Protection, Health and Safety, Anti-Bullying and IT policies.

  **iv.** The e-Safety Policy will be reviewed annually in September.

4. **Teaching and learning**

  a. Why internet use is important

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

5. **Internet use will enhance learning**

- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what internet use is acceptable and what is not, and given clear objectives for internet use.
- Internet access will be planned to enrich and extend learning activities.

- Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

## 6. Pupils will be taught how to evaluate internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Head of ICT.
- Staff should ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

## 7. Managing Internet Access

a. Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses a fibre connection with a firewall and filtering.

b. Email

- Pupils may only use approved email accounts on the school system. Children are not allowed access to personal email accounts or chat rooms whilst in school. Children are prevented from sending or receiving mail outside of the school domain.
- Pupils must immediately tell a teacher if they receive an offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- The forwarding of chain letters, inappropriate messages, images or videos is not permitted.

c. Published content and the school website

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The relevant heads of sections will take overall editorial responsibility and ensure that the content is accurate and appropriate

d. Publishing pupils' images and work

- Only photographs of pupils with parental permission on file may be published on the school's social media.
- Pupils' full names will not be used anywhere on the website. A child's name may be used in a social media post as long as there is no accompanying photograph, i.e. photo or name of child, never both together.
- A pupil's work can only be published with the permission of the pupil and parents.

### e. Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils are advised to never give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, email address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.

### f. Managing filtering

- The school will work in partnership with the service provider to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the IT Systems Manager or member of the department.
- Senior staff will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

### g. Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the internet.
- External IP addresses should not be made available to other sites.
- Pupils should ask permission from the supervising teacher before making or answering a video conference call - such calls should be prearranged and under the supervision of a member of staff.
- Videoconferencing should be supervised appropriately for the pupil's age.

### h. Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff have access to a school phone where contact with pupils is required.

i. Protecting personal data

- Personal data will be recorded, processed, transferred and made available in line with our Data Protection Policy

## 8. Policy Decisions

a. Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted internet access.
- All staff, including Teaching Assistants and support teachers must read and sign the IT Acceptable Use Policy (AUP) before using any school IT resource.
- At FS/Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents and pupils will be asked to sign and return a consent form agreeing to comply with the school's Internet Acceptable Use Policy.

b. Assessing risks

- In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school will 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 possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access. Similarly, should any pupil download inappropriate material at home to their phone/ ipad/ laptop and bring into school and share with others, the school cannot be held to account. Such instances would be dealt with robustly and in line with the school's Behaviour Policy regarding serious instances of inappropriate behaviour.
- The ICT teacher and the Head of Humanities/ ICT will ensure that the e-Safety Policy is implemented and compliant with the policy monitored.
- The school's filtering systems specifically identify terms relating to radicalisation, and detected instances are monitored and reported, in line with the school's Safeguarding policy.

c. Handling e-Safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Principal
- Complaints of a child protection nature must be dealt with in accordance with the school's child protection procedures.
- Sanctions within the school discipline policy include:
  - interview/counselling by class teacher / Head of Section/ Principal
  - informing parents or carers;

- removal of internet or computer

d. Community use of the Internet

- The school will be sensitive to internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

## 9. **Communications Policy**

a. Introducing the e-Safety policy to pupil

- Rules for internet access will be posted in all networked rooms.
- Pupils will be informed and regularly reminded that internet use will be constantly monitored.
- Advice on e-Safety will be introduced at Year 1 level to raise the awareness and importance of safe and responsible internet use and will continue in all year groups as a matter of course. Safe usage must be embedded in the school's way of life for all pupils and staff.

b. Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

c. Enlisting parents' / carers' support

- Parents' / carers' attention will be drawn to the School's Internet Acceptable Use policies.

## **Appendix 1: Internet use - Possible teaching and learning activities**

| **Activities** | **Key e-safety issues** | **Relevant websites** |
|---|---|---|
| Using search engines to access information from a range of websites. | Pupils should be supervised.<br>Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with. | Web quests e.g.<br>Ask Jeeves for kids<br>Yahooligans<br>CBBC Search<br>Kidsclick<br>Picsearch<br>safesearch |

| | | |
|---|---|---|
| Exchanging information with other pupils via email. | Pupils should only use school email accounts.<br>Pupils should never give out personal information.<br>Shared files/folders. | Ms Teams |
| Publishing pupils' work on school and other websites. | Pupil and parental consent should be sought prior to publication.<br>Pupils' full names and other personal information should be omitted. | School website<br>School social media accounts. |
| Publishing images including photographs of pupils. | Parental consent for publication of photographs should be sought - consent withheld list is maintained.<br>Photographs should not enable individual pupils to be identified.<br>File names should not refer to the pupil by name. | School website<br>School social media accounts. |
| Communicating ideas within chat rooms or online forums. | Only chat rooms dedicated to educational use and that are moderated should be used.<br>Access to other social networking sites should be blocked.<br>Pupils should never give out personal information. | |
| Audio and video conferencing to gather information and share pupils' work. | Pupils should be supervised.<br>Only sites that are secure and need to be accessed using an email address or protected password should be used. | |

This Policy must be read in conjunction with the following policies:

Bullying and prejudice policy

Child protection and safeguarding policy

Behaviour management policy

| | |
|---|---|
| Reviewed: | 29 September 2022 |
| To be reviewed: | Annually by 30th September |
| Responsibility: | IT technician/ ICT teacher and Head of Humanities and IT |