

ICT and Internet Safety Policy

Introduction

The ICT policy of BIPS aims to:

1. Promote the use and development of ICT at BIPS.
2. Ensure that all staff, pupils and parents understand and agree on the approach to ICT at BIPS.
3. Improve and enhance teaching and learning at BIPS.

The development and expansion of ICT and particularly of the internet, has transformed learning in school in recent years. Students will need to develop high level ICT skills, not only to maximize their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment.

Aim

- The school shall protect and educate pupils and staff in their use of technology.
- The School shall have the appropriate mechanisms to intervene and support any incident, where appropriate.
- The School shall audit the training needs of all staff and provide training to improve their knowledge of and expertise in the safe and appropriate use of new technologies.
- Work closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at school
- Use pupils' and families' views more often to develop e-safety strategies
- Manage the transition from locked down systems to more managed systems
- To help pupils understand how to manage risk; to provide them with richer Learning experiences and to bridge the gap between systems at school and the more open systems outside school
- Provide an age-related, comprehensive curriculum for e-safety that enables pupils to become safe and responsible users of new technologies
- Work with their partners and other providers to ensure that pupils who receive part of their education away from school are e-safe
- Systematically review and develop their e-safety procedures, including Training, to ensure that they have a positive impact on pupils' knowledge and understanding.

Risk factor

However the use of new technology can put students at risk within and outside the school. Some of the risk factors are

- Access to illegal ,harmful or inappropriate images or contents

- Unauthorized access to loss of /sharing of personal information.
- Access to unsuitable video/internet games
- Cyber bullying
- Illegal downloading of music or videos
- Inappropriate communication/contact with others, including strangers
- The potential for excessive use which may impact on the social and emotional development and learning of the young persons.

Many of these risks reflect situation in the off line world and it is essential that this ICT policy is used in conjunction with other school policies.

Policy

Acceptable use - Computers and Internet

- Access to the Internet is specifically limited to activities in direct support of official School activities
- In addition to access in support of specific work related duties, the BIPS Internet connection may be used for educational and research purposes.
- If any user has a question of what constitutes acceptable use he/she should check with their supervisor for additional guidance. Management or supervisory personnel shall consult with IT Coordinator for clarification of these guidelines.

Inappropriate use – Computers, Internet and Website

- Internet access shall not be for any illegal or unlawful purpose. Examples of this are the transmission of violent, threatening, defrauding, pornographic, obscene, or otherwise illegal or unlawful materials
- The Internet shall not be accessed for private, recreational or any non-BIPS- related activity.
- The BIPS's intranet or Internet connections shall not be used for commercial or political purposes.
- Employees shall not use BIPS network for personal gain. Internet access through the BIPS network shall not be for or by performing unauthorized work for profit.
- Users shall not attempt to circumvent or subvert security measures on either the BIPS's network resources or any other system connected to or accessible through the Internet.
- BIPS employees shall not use Internet access for interception of network traffic for any purpose other than engaging in authorized network administration.
- BIPS users shall not make or use illegal copies of copyrighted material, store such material on BIPS equipment or transmit such material over the BIPS network.

Procedure

- When accessing the internet students will make use of the school websites, 'kid safe' search engines or sites and URLs approved and provided by the teacher. Students must only use the internet for teacher approved purposes.
- Students and staff will have ongoing learning related to appropriate and safe ICT usage that engages in powerful learning opportunities and minimizes and manages risk.
- Students will use internet capable devices with the specific guidance and support of their teacher.
- Teachers will be aware of what their students are doing on the devices and will monitor them as appropriate.
- All student work that is to be shared (printed, emailed, blogged etc.) must be seen and approved.
- By the teacher and not breach copyright law users other than staff and students will only use the internet through the agreement of the principal/deputy principal/ICT leader and will follow the same guidelines as for staff/children

Dissemination

The Principal must:

- Ensure that the safeguarding and child protection policy and procedures are implemented and followed by all staff
- Allocate sufficient time and resources to be enabled to carry out their roles effectively, including the assessment of pupils and attendance at strategy discussions and other necessary meetings
- Ensure that all staff feel able to raise concerns about poor or unsafe practice and that such concerns are handled sensitively and in accordance with the school's whistle blowing procedures
- Ensure that child's safety and welfare is addressed through the curriculum.

Computer and Internet usage - Conclusion

All terms and conditions as stated in this document are applicable to all users of the BIPS network and the Internet. These reflect an agreement of all parties and should be governed and interpreted in accordance with the school regulation.

User compliance

The user must abide by the BIPS computer, network, and Internet use policies. Any violation of this policy is considered unethical and may constitute a criminal offense. If you commit any violation, your access privileges may be revoked and disciplinary action or appropriate legal actions may be taken.