Achieving Excellence Together

iBOS ICT & E-Safety Policy

The aims of our school are

- A school where teachers, staff, and students are expected to support and extend the atmosphere of respect, courtesy, the love of learning and the value of friendship that is held dear at iBOS.
- iBOS aims to develop students to become well-rounded individuals. We aim to empower our students with the best tools and resources, making them capable in following and achieving their dreams, to become valued members of our global societies, and to allow them to make a positive difference to the world, wherever they choose to progress to.
- Students leave iBOS prepared for university. They are confident, contributing and caring members of the global community and they have embraced the challenge of our specialised education. They will have gained the values that equip them to make a positive contribution

Responsibility of: The Principal

Date Ratified: 05 May 2023

Review Date: 05 May 2024

iBOS ICT and E-Safety Policy

The overall aim of Information and Communication Technology is to enrich learning for all pupils and to ensure that teachers develop confidence and competence to use Information and Communication Technology in the effective teaching of their subject. Information and Communication technology offers opportunities for pupils to:

- Develop their ICT capability and understand the importance of information and how to select and prepare it.
- Develop their skills in using hardware and software to enable them to manipulate information.
- Develop their ability to apply ICT capability and ICT to support their use of language and communication.
- Explore their attitudes towards ICT, its value for themselves, others and society, and their awareness of its advantages and limitations.

Develop good Health and Safety attitudes and practices.

Access to the school's systems

Students will use the school's systems for their daily lessons, and to review recordings of lessons.

Students will have their own login and accounts which they will log into our VLE (virtual learning environment) with. They are expected to protect their password and login details and not pass these on to anyone else.

The security of the VLE will be reviewed regularly and virus protection will be updated regularly.

Students must not upload any files onto the system unless requested by their teacher.

Students will be provided with a school email which they will need to upload homework and communicate with the school. This email must not be used for any other purpose.

The school must be made immediately aware if a student starts to receive spam emails.

Security and Privacy

Students must not pass any personal details over the schools' systems. All details such as their address must be kept private.

Students must not attempt to bypass or interfere with any setting on the school's systems. Doing so may lead to action being taken against them.

Monitoring

Departmental monitoring is carried out by the analysts. There is an annual review of this policy. Monitoring is carried out in the following ways

- Informal discussion between students and teachers
- Observation by the analysts of the student screens

What is E-Safety?

The use of the Internet as a tool to develop learning, understanding and communication has become an integral part of school and home life. There are always going to be risks in using any form of communication that lies within the public domain, therefore there must be clear rules, procedures and guidelines to minimise those risks whilst children and staff use these technologies. Whilst iBOS acknowledges that we will endeavour to safeguard against all risks, we may never be able to completely eliminate them. Any incidents that may arise will be dealt with quickly and according to our policy to ensure students continue to be protected.

Roles and responsibilities

It is important to emphasise that we are all responsible for E-Safety and our specific responsibilities are outlined below:

Governors

- It is their overall responsibility to ensure that there is an overview of E-Safety (as part of the wider remit of Safeguarding Child Protection) across the school and that they promote and report on E-Safety developments and their links with the school development plan/ICT development plan, safeguarding child protection, and other policy changes.
- The Governing Body has appointed an E-Safety governor who will challenge the school about having appropriate policies, procedures, staffing responsibilities and ICT security systems.

Network Manager

- Implements agreed on policies, procedures, staff training, and curriculum requirements and takes a responsibility for ensuring E-Safety is addressed to establish a safe ICT learning environment.
- Ensures that all adults in the school and parents are aware of the filtering levels and why they are there to protect students.
- Ensures that the filtering levels on all equipment are appropriate for our students and are set at the correct level.
- Ensures that any concerns are reported to the designated safeguarding lead.
- Keeps a log of incidents for analysis to help inform future development and as part of the school's safeguarding procedures.
- Ensures there is appropriate anti-virus software and anti-spy software in place on all school equipment and that this is reviewed and updated regularly.
- Reports accidental access to inappropriate materials to the ICT technical manager of the ISP and or filtering service so that inappropriate sites are added to the restricted list.
- Has responsibility for the transparent monitoring of the Internet and online technologies. For example, any student or staff files may be accessed by the network manager if it appears that the E-Safety policy may have been breached, on the authorisation of the

Designated Safeguarding Lead or the Head or if it involves the Head, the Chair of Governors.

All staff

- Should acknowledge that they have read, understood and agreed with the Staff Code of Practice. They will know that by following the rules they are safeguarded from allegations and that they understand their responsibilities to safeguard students when using online technologies. They have a password to access a filtered Internet service and know that this should not be disclosed to anyone, nor should they leave a computer or other device unattended whilst they are logged in.
- When accessing the school system from home, the same Code of Practice will apply.
- Staff should request training or access internal training so that they are updated on new and emerging technologies. They should keep up-to-date with E-Safety knowledge that is appropriate for the age group they teach and reinforce it through their curriculum.
- Ensure the correct procedure is used for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.
- Ensure that students are protected and supported in their use of online technologies and are taught to use them safely and responsibly so that they can be in control and know what to do in the event of an incident.
- To work closely with tutors and pastoral leaders regarding PSHE so that students are taught about and encouraged to consider the implications of misusing the Internet, for example posting inappropriate material to websites, which can have legal implications.
- Staff are expected to be aware of and adhere to data protection rules when communicating by email and also the age-appropriateness and legalities of the resources they use and upload.
- They must report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies to the Deputy Head and, if necessary, complete the appropriate logs of concern or discussion.

Students' responsibilities

- Students will fully participate in the E-Safety curriculum provided in ICT and PSHE lessons.
- Students are expected to use the Internet and other ICT e.g. mobile phones, digital cameras, and webcams, safely and responsibly at all times in school.
- Students are responsible for following the E-Safety code of conduct for students whilst within the school.
- Students know that cyberbullying or posting of unauthorised content or malicious comments to or about other pupils or staff, is an extremely serious offence and the consequences would be enforced as per the Behaviour Management flowchart and Anti-Bullying Policy.
- Students should never bring the School into disrepute with regards to their digital use.
- Students are taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away and will be expected to do so knowing that they will not be reprimanded for behaviour that is not their responsibility.

Parents/carers

- All parents and carers have access to this policy via the School website.

- Parents/carers and students are asked to read the E-Safety code of practice to understand the implications for students if there should be any misuse of technologies.
- Are encouraged to seek advice and support from the school where necessary by contacting their child's Form Tutor or the Deputy Head