E-Safety Policy

E Safety Policy

This policy is applied for Staffs -Teaching and Non-Teaching, Students, Parents/Caregivers and Visitors to protect the interests and safety of the whole school community. Our e-Safety policy has been agreed by the Senior Management Team and Staff. The eSafety policy and its implementation are reviewed annually. This is to ensure that all users will receive regular information and training on e-Safety issues through the coordinator at scheduled intervals. All Governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Internet Usage Policy (General)

The following activities are strictly forbidden on School Network:

- Illegally downloading music, films, software, and other digital goods (Piracy)
- Installing software on School computers without the authorization of a School Information technology, IT representative
- Gaining unauthorized access to programs, systems, websites. (Hacking)
- Introducing malicious software (Malware) onto the School network or performing other actions that put the security of the organization at risk
- Attempting to bypass the School web filter to access blocked material
- Accessing content that would reasonably be considered not safe for work such as pornography, violent imagery, and other adult-oriented content.
- Sharing or leaking passwords or other credentials that are used to provide access to company equipment, services, accounts, and other company assets.
- Excessive personal use of company internet during work hours is not permitted
- Personal use of the internet during work hours-Staffs are expected to use School provided internet and other devices as a resource for completing their assigned duties and supporting the objectives of SBIS
- Sharing confidential material, trade secrets, or other proprietary information outside of authorized parties of the School

Managers and Leaders

- Ensure the whole school community is aware of what is safe and appropriate online behaviour and understand the sanctions for misuse
- All Staff should be given the opportunity to help contribute to and shape online safety policies and procedures

- Review any reported online safety incidents to inform and improve future areas of teaching, training and policy development
- Take appropriate action in line with child protection policies and procedures, if the filtering system and monitoring approaches identify any causes for concern.
- Ensure the positive social values consistently communicated across the school in order to encourage online behavioural expectations

Online Safety Lead/ E-Safety Coordinator

- Ensure policies and procedures that incorporate online safety concerns are in place. This should include but is not limited to; Acceptable Use Policies (AUPs), mobile phones, peer on peer abuse (including responses to cyberbullying and sexting) and social media.
- Ensure there are robust reporting channels and signposting to internal, local and national support.
- Record online safety incidents and actions taken, in accordance with the school's normal child protection mechanisms.
- Ensure the whole school community is aware of what is safe and appropriate online behaviour and understand the sanctions for misuse.
- Liaise with the local authority and other local and national bodies as appropriate.
- The use of portable media such as memory sticks and CD ROMS will be monitored closely as potential sources of computer virus and inappropriate material.

Teaching and Support Staff

- Use sensible email addresses, usernames and strong passwords rather saving on browser. Consider your own digital identity and security.
- Don't put anything online that you wouldn't want your friends, family, colleagues, and employers to see. Protect your own digital reputation.
- Staff will use a school phone where contact with pupils is required.
- Students will use teams private chat to conduct hate speech/bullying. Supervised chat allows teachers to see the chat between students and allows them to block communication between certain students as well as to ensure a safe learning environment.

Students

- Students are not allowed to bring personal mobile devices/phones to school.
- Any phones that are brought to school are sent to the school office and kept there until the end of the day.
- The sending of abusive or inappropriate text messages or emails outside school is forbidden.

Parents/Caregivers

Parent's concern is increasing around online risks, perhaps due to media coverage & pace of change of technology. Also, they must ensure that,

- Proper Parental controls are applied on home broadband router.
- Content lock on mobile networks.
- Safe search on Google (& other browsers) & YouTube; child –friendly search engines

Your children will be watching the way you use technology and they will copy. Make sure there is some consistency in how your role model good behaviour.

Infrastructure- Equipment, Filtering and Monitoring

- Ensures network healthy through use of Sophos anti-virus software and network set-up so staff and pupils cannot download executable files
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved learning platform
- School ICT systems capacity and security will be reviewed regularly

Acceptable Use Policy

This policy provides rules for the acceptable use of personally owned devices on the school network. This policy applies to all employees and any other person using or accessing information or information systems. Exception to this policy must be approved by the designated representative.

Users that wish to access the network using their personally owned computer may do so using only - authorized software and only with the approval of the user's supervisor and the IT department. Users must follow the same rules when accessing the network from both school-issued equipment and personally owned devices. When connected to the network, the user will NOT: -

- Use the service as part of violating the law
- Attempt to break the security of any computer network or user
- Attempt to send junk email or spam to anyone
- Attempt to send a massive amount of email to a specific person or system in order to flood their server

IT reserves the right to determine the level of network access for each personally owned device. The user could be granted full, partial or guest access.

IT reserves the right to block or limit the use of certain third-party applications, such as those that probe the network or share files illegally, that may harm the corporate network.

As the number of approved applications continually evolves, the user must check with the IT department for the current list of approved third-party applications and get IT approval before downloading it on the device.

While does not own the device, they do own all school data. Therefore, reserves the right to remotely wipe the user's personally owned device at any time. Not only will school data get wiped, but the user's personal data could be lost as well. The user must understand and accept this risk.

Bring Your Own Device (BYOD) Policy

Refers to employees taking their own personal device to work, whether laptop, smartphone, or tablet, in order to interface with the internal/participant organization's network resources. This also refers to mobile storage devices such as USB drives, external hard drives, etc.

- All personally owned devices must be registered with the IT Department
- Password protect all personally owned devices
- Do not leave personally owned device unattended

IT will support personally owned devices as follows-

- The user will be required to allow IT to load security software on each device
- The user will be required to allow IT to install remote wiping software on each device
- Upon request the IT will install the necessary software's/apps.

Personal Data Protection Policy

- The school will use information about students to further curriculum, professional and managerial activities in accordance with the business of the school and will contact the parents or guardians, if it is necessary, to pass information beyond the school.
- The school will hold personal information on its systems for as long as individual members of staff remain at the school and remove it in the event of staff leaving or until it is no longer required for the legitimate function of the school.
- We will ensure that all personal information supplied is held securely.
- Each teacher has the right to view personal information that the school holds and to have any inaccuracies corrected.

Social Media Policy

Sometimes people hide behind fake profiles for dishonest reasons. Agree how they will respond to requests from people they don't know in real life. We must ensure that the below things are properly defined.

- Never ever to meet up with anyone they don't know in real life
- Set up safe social media profiles that don't share personal information
- Turn off geo location settings on devices
- Use the strongest privacy settings on social media
- Learn how to report / block/ mute

Incident Handling

Incident reporting and handling process within the school are updated to address incidents related to BYOD devices including but not limited to lost, stolen, unauthorized access, breach of policy etc. All employees are aware of incident reporting procedure related to Cyber Bullying,