



E–Safety Policy

2023 – 2024

Approved by: Mr Mohsin Ibrahim

Date of review: September 2023

Next review date: September 2024



Scope of the Policy

This policy applies to all members of the school (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these Powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour (ADAB) Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / caregivers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school: Local Advisory Board:

LAB members are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the LAB members receiving regular information about e-safety incidents and monitoring reports. A member of the LAB has taken on the role of E-Safety member. The role of the E-Safety member will include:

- Regular meetings with the E-Safety Coordinator.
- Regular monitoring of e-safety incident logs.
- Regular monitoring of filtering / change control logs.
- Reporting to relevant members / Board / Committee / meeting.

Principal and Senior Leaders:

- The Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community.
- The Principal and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Principal and Senior Leaders are responsible for ensuring that the E-Safety Team and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Principal will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.



E-Safety Coordinator:

- Leads the e-safety committee.
 - Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.
 - Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
 - Provides training and advice for staff.
 - Liaises with the MOE / relevant body.
 - Liaises with school technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets regularly with E-Safety LAB member to discuss current issues, review incident logs and filtering / change control logs.
- Attends relevant LAB meeting.
- Reports regularly to Senior Leadership Team.

Network Manager / Technical staff:

The Director of Digital & IT is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack • That the school meets required e-safety technical requirements and any MOE / other relevant body E-Safety Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- The filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head of Year / Principal / Senior Leader; E-Safety Coordinator.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school / academy e-safety policy and practices
- They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP) • They report any suspected misuse or problem to the Head of Year for investigation / action / sanction • All digital communications with students / parents / carers should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities • Students understand and follow the e-safety and acceptable use policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations



- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection / Safeguarding Designated Safeguarding Lead

Should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Students:

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realize that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Caregivers:

Parents / Caregivers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and caregivers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website / blog
- Their children's personal devices in the school (where this is allowed)

Community Users

Community Users who access school systems / website as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.



Policy Statements

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognize and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents / Caregivers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and caregivers through:

- Curriculum activities.
- Letters, newsletters, website.



- Parents / Caregivers evenings / sessions.
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications.

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school / academy website will provide e-safety information for the wider community.
- Supporting community groups (e.g. Early Years Settings, Childminders, youth / sports / voluntary groups) to enhance their e-safety provision.

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced.