مدرسة جيمس متروبول
GEMS Metropole School
MOTOR CITY

Discover LEADERSHIP

E–Safety of Policy
2023 – 2024

Approved by:	**Mr. Naveed Iqbal**
Date of review:	**October 2023**
Next review date:	**October 2024**

GEMS EDUCATION
We see *genius* in every child

Overview

GEMS Metropole School Motor City is dedicated to cultivating a 21st-century learning environment, aiming to ensure fair access to technology that empowers students to become self-directed learners, collaborative team players, and adept producers and consumers of information. The integration of digital technologies into teaching and learning is strategically designed to enhance student learning through both internal resources and the effective utilization of a broader range of online tools. Internet access is considered a privilege for students who demonstrate a responsible and mature approach to its use. GEMS Metropole School Motor City is committed to providing students with secure and supervised Internet access as an integral part of their educational journey.

Rationale

Teachers actively incorporate innovative technology into their lesson plans to deliver high-quality teaching and learning experiences. Concurrently, they prioritize online safety to ensure a secure digital environment for students. The school adopts a comprehensive approach to internet safety, fostering a culture of responsible digital citizenship through shared policies, guidance, continuous training, and professional development for all staff members. This commitment extends to supporting best practices and promoting safer online engagement for the entire GEMS Metropole community, including non-teaching staff and parents.

Intent

This policy sets out the school's approach to internet safety as part of the GEMS network of schools, how we ensure that online safety is our top priority and how we engage and support our community to maintain, develop and promote safer practice.

Roles and Responsibilities

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

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 the safeguarding 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
- Senior leaders must ensure that appropriate training is given to staff to ensure they know the steps to take in the event of a serious e-safety breach

Network Manager / Technical staff:

The IT technician 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 KHDA / 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 Senior Leadership Team.

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 such as Safer Internet Day
- 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)

Communications

A wide range of rapidly developing communications technologies has the potential to enhance

learning. When using communication technologies, the school considers the following as good

practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access)
- Users must immediately report, to the nominated person – in accordance with the school / academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and students or parents / caregivers' (email) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications
- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

Mobile Device Management System

All students with a device in school from Years 2-11 must be enrolled to the school's mobile device management system. The system ensures that students only have access to applications during the school day which are linked to their learning. The mobile device management system also gives teachers oversight into what students are accessing during lesson time, providing an additional layer of safeguarding alongside the school's filtering systems and app restrictions.

Recording of E-Safety Incidents

E-safety incidents are reported through the school's safeguarding (Guard) and behaviour management system

(Go4Schools). Incidents are reviewed in the weekly Safeguarding meetings. Parents are contacted alongside the report being logged in to ensure they are aware of any E-safety breaches.

This policy is the result of a review of several existing policies and is to be considered in conjunction with the following policies:

a. Safeguarding Policy
b. Anti – Bullying Policy
c. Behaviour Policy
d. Health and Safety Policy
e. BYOD Policy

Monitoring Arrangements

The school's arrangements for managing access to education and training providers for students are monitored by Mr. Nizar Mourad – School Operations Manager.

This policy will be reviewed by Neil Corrigan (DHT Primary), Joe Gannon (DHT Secondary) and Brynn Cooper (Assistant Head Teacher) annually.

At every review, the policy will be approved by Mr. Naveed Iqbal – Principal and CEO