E-Safey Policy

Published Date:	**August 2025**
The Policy will be reviewed annually, or more regularly, in the light of any significant new developments. The next anticipated review date will be:	**August 2026**

Rationale

At GFM, our approach is guided by *Grow ◌ Flourish ◌ Mindful*. Technology has transformed the way we learn, communicate, and connect with the wider world. While these opportunities are invaluable, they also present risks that could impact the safety, wellbeing, and development of our students.

The rationale for this E-Safety Policy is to establish a clear framework that protects students from online harm, ensures responsible use of technology, and supports our wider safeguarding responsibilities. By embedding safe and mindful digital practices, we prepare our students not only to succeed academically but also to make positive, responsible contributions to the communities they are part of.

Purpose

The purpose of this policy is to:

- Safeguard students from harmful or inappropriate online content, interactions, and behaviours.
- Promote responsible and ethical digital citizenship across the whole school community.
- Provide clear expectations for the safe and appropriate use of technology by students, staff, and parents.
- Ensure robust filtering, monitoring, and reporting systems are in place, supported by human oversight, to protect against online risks.
- Address the four categories of online risk — Content, Contact, Conduct, and Commerce — as well as emerging risks from artificial intelligence, mobile technology, and social media.
- Align with UAE regulations, GEMS Education policies, and The GFM Way, ensuring our digital environment reflects our values and vision.

Through this policy, we aim to enable our students to grow in confidence, flourish in a connected world, and remain mindful of the choices they make online.

Online risks for children are categorised as:

Content: exposure to illegal or harmful material such as pornography, racism, misogyny, self-harm, suicide, radicalisation, extremism, misinformation, disinformation, and conspiracy theories.
Contact: harmful interactions with others, including peer pressure, targeted advertising, or grooming.
Conduct: harmful online behaviours such as the consensual and non-consensual sharing of explicit images, online bullying, and accessing or distributing pornography.
Commerce: risks linked to online gambling, phishing, financial scams, and inappropriate advertising.

Roles and Responsibilities

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

Governors:
Governors 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 Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken the role of E-Safety Governor (or LAB sub-committee that this falls under). The role of the E-Safety Governor will include:

- Regular meetings with the assistant headteacher (AHT)/E-Safety Coordinator
- Regular monitoring of e-safety incident logs
- Regular monitoring of filtering / change control logs
- Reporting to relevant LAB /LAB Sub-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 Coordinator 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

Relevant Leader responsible for E-Safety:

- Is L2/L3 Safeguard trained
- Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Provides training and advice for staff
- Liaises with safeguarding team accordingly
- Liaises with school technical staff
- Attends relevant meetings
- Reports regularly to Senior Leadership Team
- Ensure the education around E-Safety addresses the four categories of online risks.

IT Manager / ICT Support Team:

The Co-coordinator for ICT / Computing 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, 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
- They report any suspected misuse or problem to the Head of Year for investigation / action / sanction. If the content is deemed of a safeguarding concern, then the teacher is to report this immediately as per safeguarding protocols.
- 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
- Staff should inform and educate students about the risk attached to publishing their own images on the internet e.g. on social networking sites

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 realise 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
Parents and caregivers play a crucial role in ensuring that children understand the importance of using the internet, mobile devices, and digital technologies appropriately and safely. While many parents may have only a limited understanding of e-safety risks, they remain essential partners in educating and guiding their children, as well as monitoring and regulating online behaviour. The school will support parents and caregivers by providing regular information, awareness, and guidance through:
- Curriculum activities
- Parent sessions and webinars
- High-profile events and campaigns (e.g. Safer Internet Day)
- Letters, newsletters, and the school website
-

Parents and caregivers will be encouraged to actively 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 parent sections of the website / blog
- Their children's personal devices in school (where permitted)

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. Nurseries, Childminders, youth / sports / voluntary groups) to enhance their e-safety provision

Education & Training – Staff

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. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process
- All new staff should receive e-safety training as part of their induction programme (this can fall within safeguarding and curriculum induction), ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days
- The E-Safety Coordinator (other relevant leader) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / e- safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the KHDA or other relevant organisation
- Participation in school training / information sessions for staff

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the

above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school / academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school / academy technical systems and devices
- The Principal / LA officer is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations
- Internet access is filtered for all users
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement
- An appropriate system is in place (to be described) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed)
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Artificial Intelligence (AI) and Emerging Technologies

The policy acknowledges the risks associated with artificial intelligence. Students must not use AI tools to access or generate harmful content. Staff must ensure that AI technologies used in school are safe, age-appropriate, and compliant with data protection and safeguarding requirements. The school will remain alert to risks of AI misuse, such as generating inappropriate material, misinformation, or deepfakes.

Filtering and Monitoring

The school has implemented a Chromebook-only device policy for Years 5–13 to strengthen and enhance filtering and monitoring. The school will maintain appropriate filtering and monitoring systems on all devices and networks to prevent access to harmful or inappropriate content, including scam platforms and inappropriate advertising. These systems will be regularly reviewed to ensure they remain effective, proportionate, and age-appropriate. Monitoring will combine automated tools with human oversight to ensure that safeguarding concerns are identified and addressed promptly.

The school will ensure that all AI and digital monitoring tools are configured to block access to inappropriate, harmful, or illegal material. Students and staff must not attempt to bypass, disable, or interfere with filtering systems. AI tools must not be used to generate, share, or

access offensive or harmful content. Filtering systems will be supplemented by staff moderation to maintain a safe and secure digital learning environment.

Safeguarding and Monitoring

The school will implement robust filtering and monitoring systems across all devices and networks to protect children from harmful or inappropriate online content. All automated systems will be supported by human supervision and intervention, ensuring that professional judgement remains central to safeguarding practice. School has a "whitelist" Policy for KS3 as part of the school BYOD Program. Staff and parents are responsible for requesting sites needed for educational objectives and similarly report any issues that may come to their observation.

Cyberbullying and Child-on-Child Abuse

The school will actively educate students, monitor appropriately, and respond to all forms of cyberbullying. Students must not use technology for bullying, harassment, or creating hostile online environments. The policy also recognises the risks of child-on-child abuse online, including the sharing of explicit images, and outlines clear reporting and response procedures in line with safeguarding policies.

Communication Protocols

Online communication between staff and children must only occur where necessary for the purpose of coordinating an aspect of education on our approved platforms; google classroom. All communication must take place via school devices and GEMS-approved mail servers. Communications must be transparent, professional, and available on request to the Senior Leadership Team (SLT). Staff must follow the Safer Working Practice Guidance.

Privacy and Data Security

All data collected through filtering and monitoring systems will be securely stored and protected in line with data protection regulations. The school will ensure a clear and transparent consent process is in place where personal data is collected for safeguarding purposes. Students and staff must not use AI or monitoring tools to collect, analyse, or share personal data.

Digital Footprint

The development of digital imaging technologies has created significant benefits to learning. However, staff, parents / caregivers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

Images and Recording

Any publishing of images must comply with the Safer Working Practice Policy, safeguarding procedures, and the GEMS Code of Conduct.

Images of students must only be taken on school equipment; the use of personal devices by staff for this purpose is strictly prohibited. Students must not use school devices or personal devices to take, share, or publish images or recordings of other students.

Any misuse of images or recordings, including sharing via social media, messaging platforms, or AI tools, will be treated as a serious breach of the E-Safety Policy and addressed under the Behaviour, Safeguarding policies (as well as GEMS Code of Conduct and Disciplinary policy for staff).

Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or KHDA liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk
- School staff should ensure that:
- No reference should be made in social media to pupils, parents / caregivers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or KHDA
- Security settings on personal social media profiles are regularly checked to minimize risk of loss of personal information

Incidents of misuse

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Depending on the level of misuse, this may go through the safeguarding team (for students) and could result in a sanction, and for staff, this could result in a disciplinary in line with the appropriate policy.

Please read this policy alongside:
Anti-Bullying Policy, Inclusion Policy, Safeguarding Policy, BYOD Policy, AI Policy, Parent & Student Cybersecurity Guide, Acceptable Use Policy, Policy for Data Protection and Processing, GEMS Code of Conduct, Remote Learning Protocols, Guidance for Safer Working Practice, GEMS IT policies, Behaviour Policy, Social Media Policy, Curriculum Policy and Teaching & Learning Policy