E-safety Policy

Vision: *Grow - Flourish - Achieve*
Mission: *Growing Flourishing Achievers through an innovative and sustainable learning environment that fosters academic excellence with holistic development.*

What is E-safety

E-safety is often defined as the safe and responsible use of technology. This includes the use of the internet and also other means of communication using electronic media
(E.g. text messages, gaming devices, social media, email etc). In practice, e-safety is as much about behaviour as it is electronic security.

Scope of the Policy

This policy should be read in conjunction with the following polices:

- GFA Behaviour Policy
- MoE Distance eLearning Behaviour Policy
- Safeguarding and Child Protection Policy
- GEMS Acceptable Use Policy
- GFA Inclusion Policy
- GFA Teaching and Learning 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 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.

Purpose

This E-Safety policy enables our school to create a safe e-learning environment that:

- protects children from harm
- safeguards staff in their contact with pupils and their own use of the internet
- ensures the school fulfils its duty of care to pupils
- provides clear expectations for all on acceptable use of the internet.

Why the Internet is Important

- The Internet is an essential element for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory UK curriculum and a necessary tool for learning for staff and pupils.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use. Internet use will enhance learning.
- The school Internet access is designed for pupil use and includes filtering appropriate to the age of pupils.

What are the risks

(As published by EU Kids Online 2020)

- Content; what children and young people see online
- Contact: who they communicate with online
- Conduct; how they act online

These can create a range of harmful behaviours that include:

- Online bullying and aggressive contact
- Access to inappropriate or illegal online content
- Online sexual predation
- Youth produced sexual imagery (sexting)
- Self-harm
- Identity theft
- Over-engagement with technology E.g. gaming, social media, screen time
- Extortion
- Privacy
- Commercialisation and the impact of media on self-image and identity

Roles and Responsibilities

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

Governors:

Local Advisory Board 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 Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body (Local Advisory Board) has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- Regular meetings with the Pastoral Team
- Regular liaison with the school and parents
- Reporting to relevant Governors / 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 Digital Safety DDSL 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

Digital Safety DDSL

- 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 school technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Meets regularly with the IT Engineer to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant meeting / committee of Governors

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

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

ICT Engineer/Technical staff:

The ICT engineer 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 ADEK / 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 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

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 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 / newsletter
- 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.

Infrastructure

Acceptable Use of Technology

Technical – 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 meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school's 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's technical systems and devices
- The Principal / ICT Engineer is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users
- School's 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, workstations, 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
- An agreed policy is in place for the provision of temporary access of "guests" (E.g., trainee teachers, supply teachers, visitors) onto the school systems
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

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 recognise and avoid e-safety risks and build their resilience.

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

- A planned e-safety curriculum is be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages are reinforced as part of a planned programme of assemblies and pastoral activities
- Students are 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 are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students are helped to understand the need for the pupil BYOD Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff 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 are 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

E-safety in KS 1

In Computing lessons, children are taught to:

- Use technology safely and respectfully.
- Keeping their personal information private.
- Identify where to go for help and support when they have concerns about the content. or contact on the internet.

E-safety in KS 2

- In Computing lessons children are taught to understand that they should never give out personal details to online friends such as: mobile number and any pictures of themselves, email address phone number, address, school they attend and parents' information (E.g., banking details).
- They Should never meet online friends.
- Help them to understand the risks of sharing pictures online
- Explain why they should not meet up with online friends
- They should not respond to spam / junk email & texts,
- People are not always reliable (who they say they are)
- Cyberbullying
- Who to talk to/report to

E-safety in KS 3

- Reiterate all aspects of E-safety topics taught in Key Stage 2
- Staying safe on Social Networking sites
- Privacy Settings
- Age restrictions
- Digital Footprints
- Digital Citizenship

- Cyberbullying
- Who to talk to/report to

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
- School newsletters
- School website
- Coffee Mornings/Webinars
- 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

Education and 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:

- All new staff should receive safeguarding and e-safety training as part of their induction programme, 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

Training – Governors

Local Advisory Board members 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 school / ADEK / or another relevant organisation
- Participation in school training / information sessions for staff

Standards and Monitoring

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's / academy's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. 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:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet E.g., on social networking sites
- In accordance with guidance from the Ministry of Education, parents / caregivers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of students are published on the school website
- Students' work can only be published with the permission of the pupil and parents or carers

Data Protection Act- Referenced in GEMS' Acceptable Use Policy

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets government requirements

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices

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

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools and local authorities 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 gender, race or disability or who defame a third party may render the school or ADEK 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 ADEK
- Security settings on personal social media profiles are regularly checked to minimize risk of loss of personal information

The school's / academy's use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Monitoring

Each class and subject teacher are responsible for monitoring their respective teams, groups and channels on a daily basis.

The Pastoral Teamand E-safety Officer will also do spot checks on a weekly basis to ensure that responsible digital citizenship is adhered to at all times.
Should any inappropriate behaviour occur – staff will follow the following procedures:

Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident.

Refer to the GFA Behaviour Policy and MoE Distance Learning Behaviour Policy.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

E-safety Behaviour Ladder – As per Ministerial Resolution No. 581

Example of Behaviour Offences (as per the Ministerial Resolution No. (581) of 2018 Concerning Students' Management)	
First Degree Offences	**First Category (minor) Violations** 1.1 Being repeatedly late to the morning parade or failing to participate therein without an acceptable excuse. Absence by more than 3% without an excuse. 1.2 Failing to attend the classes on time repeatedly without an acceptable excuse. Lack of personal hygiene (hair, nails, clothing) 2.2 Non-compliance with the school uniform or the school sports uniform without an acceptable excuse. 2.3 Overgrown hair for boys or bizarre haircuts for boys and girls. 2.4 Not brining the books and school kits without an acceptable excuse. 2.5 Non-compliance with the positive behavior rules inside and outside the classroom, such as: keeping calm and disciplined during the class time and making inappropriate sounds inside or outside the classroom. 2.6 Sleeping during the class time or formal school activities with no justification (after making sure of the student's health status). 2.7 Eating during the class times or during the morning parade without a justification or permission (after making sure of the student's health status). 2.8 Non -compliance with presenting homework and assignments given to him / her in a timely manner. 2.9 Misuse of the electronic devices such as the tablets etc., during the class, including playing games and using headphones inside the classroom. 2.10 All of what is similar to these offenses as per the discretion of the Behavior Management Committee.
Second Degree Violations	**Second Degree Offences (Medium Risk) Can be issued with internal exclusion for 1-3 days / external suspension if repeated.** Repeating the irregularities of the first Level more than 3 times 2.1 Not attending the school without an acceptable excuse at any time, including before and after the holidays and ends of weeks and before exams. 2.2 Getting in or out of the classroom during the class time without permission. 2.3 Not attending the school activities and events without an acceptable excuse. 2.4 Inciting quarrel, threatening or intimidating peers in the school. 2.5 Acting in a manner contradicting with the public morals or the public order at the school and with the values and traditions of the society, such as imitating the opposite sex in terms of clothes, appearance, haircuts and use of makeup. 2.6 Writing on the school furniture or school bus seats. Tampering with the alarm bell or the lift. 2.7 Bringing mobile phones or misuse any means of communication. 2.8 Verbally abusing or insulting students, staff, or visitors of the school. 2.9 Smoking or possessing the relevant kits inside the school campus. 2.10 Refusing to respond to the instruction of inspection or to hand over the banned materials. 2.11 All of what is similar to these offenses as per the discretion of the Behavior Management Committee
Third Degree Offences	**Third Category Violations (Serious / Dangerous) Can be issued with bus bans or external suspension.** 3.1 Various types and forms of bullying. 3.2 Copying or reproducing the assignments, reports, researches or projects and taking credit for them. 3.3 Getting out of the school without permission or absconding during the school day. 3.4 Attempting to defame peers and the school staff via the social media or abusing them. 3.5 Impersonating others' personality in the school, during transactions, or forging the school documents. 3.6 Destroying or seizing the school furniture, tools, and vandalism. 3.7 Tampering with or destroying the school buses. Causing harm to the driver, supervisor, or the other road users. 3.8 Assaulting others in the school, without causing any injuries to the victim. 3.9 Driving a private car recklessly inside or around the school campus, and not following the security and safety instructions. 3.10 Capturing, possessing, publishing or disseminating photos of the school staff and / or students without their permission. 3.11 All of what is similar to these offenses, as per the discretion of the Behavior Management Committee

Fourth Degree Offences	**Fourth Degree Offences (Very Serious) Suspension from school pending investigation.** 4.1 Using the communication means or social media for unlawful or immoral purposes, or in a manner discrediting the educational institution and its staff or others. 4.2 Possessing or using arms or blade weapons, or their equivalent inside the school. 4.3 Committing sexual assault inside the school, the bus or during activities. 4.4 Assaulting others in the school causing injuries to the victim (corporal abuse). 4.5 Systematic (pre-planned) or covering up theft. 4.6 Bringing, possessing, presenting, or promoting information or electronic materials that are unauthorized and inconsistent with the values, morals, public order, and public decency. 4.7 Sexual harassment inside the school, the bus, or during activities. 4.8 Leaking questions of the exams or engaging therein, in any way. 4.9 Setting the school campus on fire. 4.10 Abusing political, religious, or social figures in UAE. 4.11 Possessing, bringing, promoting, or using narcotics, medical drugs, or the psychotropic substances inside the school or the school bus, or being under the influence of narcotics, non-prescribed medical drugs or the psychotropic substances. 4.12 Disseminating or promoting ideas or beliefs on extremism, blasphemy or atheism, or the ones harming the political and social regulations of the society. 4.13 Disdaining the divinely revealed religions or stirring sectarian strife in the school. 4.14 All of what is similar to these offenses, which are considered as legally punishable offences, as per the discretion of the Behavior Management Committee.

In the event that a student with special educational needs or of determination commits a behavioural offence during distance learning, SLT and the school support team shall coordinate with each other to study the behaviour of the student to determine the relationship between the offence and the disability, and then apply the same measures mentioned in the 2018 Student Behaviour Management Policy.

Safeguarding Incidents

Incident Description	Action and Reporting
Sharing inappropriate or explicit images	Class teacher reports to DSL following the Safeguarding reporting procedure DSL meets with parents, records it on Guard Refer to school counsellor where appropriate
Using Teams/Phoenix Classroom after hours or late in the evenings	
Sharing personal information	
Sharing inappropriate photos of themselves	
Inappropriate use of the camera during online lessons	

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, incidents will be reported immediately to the police.

Other Incidents

All members of the school community will be responsible users of digital technologies, who understand and follow school / academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Involvement by ADEK or national / local organisation (as relevant).
- Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  Incidents of 'grooming' behaviour
  The sending of obscene materials to a child
  Adult material which potentially breaches the Obscene Publications Act
  Criminally racist material
  Other criminal conduct, activity or materials
  Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school / academy and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.

Impact

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys of reported incidents:
- Reporting records
- Lesson recordings and logs
- Meetings with students, staff, parents and governors

Monitoring and review

This policy will be reviewed and updated annually or as needed. Within school, the Senior Leadership team will report regularly to the Principal and LAB members concerning the effectiveness of the policy.

Signed .... Date 01/07/24
Principal/CEO

Next policy review date: 1 July 2025

Appendix A:
Bring Your Own Device (BYOD)/ DIgital Device Acceptable Use Agreement (DDAUA)
The completed form should be retained by the group for evidence and reference purposes.

Digital Device Acceptable Use Agreement (DDAUA)

- GEMS Founders School Masdar City recognises that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship.
- The purpose of this agreement is to establish an environment that is reliable, secure, compliant to regulatory obligations, manageable, and conducive to positive pedagogy at school from the perspective of end-user devices. This agreement is to ensure that all students use technology in school, at home and elsewhere, effectively, safely and responsibly, to facilitate learning on a 24/7 basis, and to help ensure that they develop the attributes of competent digital citizens. The rules written in this agreement are not all inclusive. GFA reserves the right to change this agreement as and when it deems it necessary to do so.
- This policy applies to all digital resources, not only the computers, devices and equipment provided in the school's IT labs, but also the personal devices students bring to school in accordance with the school's Bring Your Own Device (Year 2 – 8) Policy.
- Please refer to the complete policy on the school website.
- To use the school's digital resources, they must follow the guidelines set forth in this policy. The rules written in this agreement are not all inclusive. GFA reserves the right to change this agreement as when it deems it necessary to do so. It is a general agreement that all facilities (hardware, software, Internet, etc.) are to be used in a responsible, ethical, and legal manner, in and out of school. By using any digital resources, whether owned personally or by the school, users acknowledge their understanding of the Electronic Devices / Digital Resources / BYOD Agreement as a condition of using such devices and the Internet. The school provides some electronic devices and services to promote

educational excellence. The school has a responsibility to maintain the integrity, operation, and availability of its electronic systems for access and use. The school does not guarantee user privacy or system reliability.

- Whilst on site, access to the school network and the Internet should be considered a privilege, not a right, and can be suspended immediately, without notice. Access on site is available only for educational and administrative purposes. Digital resources are to be used in accordance with this Policy and all users will be required to comply with its regulations.
- The guidelines provided in this policy are intended to help users understand appropriate use. The school may restrict, suspend, or terminate any user's access to the school's computer systems upon violation of this Policy.
-

The **DDAUA** provides guidelines for using all digital hardware and software (on individual computers/devices, on local area networks, wide area networks, wireless networks, the Internet and companion technological equipment - e.g. printers, servers, whiteboards, projectors, etc. when students are at school). The Agreement also establishes rights and responsibilities for all users, in and out of school. All users of the school network and technological devices anytime, anywhere, are expected to follow the guidelines or risk loss of digital privileges. In cases of serious breaches, further action may be taken, in line with the school's standard disciplinary procedures.

School Network Accounts

- Accounts on the systems at GFA are considered secure, although absolute security of any data cannot be guaranteed.
- Students should not store commercial software, music, and/or games or hidden files to their school network account profile folders.
- School-related files are the only files to be saved in a school network account Profile folder temporarily and should be emailed to student personal email or saved in their fusion virtual learning environment profiles.
- Use only their account/password. This practice will ensure that only their personal device is connected to the network.

Personal Safety

- Students should not share personal information, including phone number, address, ID number, passwords or birthday over the internet without adult permission.
- Students should recognise that communicating over the internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others.
- Students should not agree to meet someone they met online in real life without parental permission.
- If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher if you're at school; parent if you're using the device at home) immediately.
- Students should always use the Internet, network resources, and online sites in a courteous and respectful manner.
- Students should also recognise that some valuable content online is unverified, incorrect, or inappropriate content.
- Should not to post anything online that they wouldn't want parents, teachers, future colleges, employers or the UAE government to see.

Equipment

- GFA encourages students the use of the latest devices as these will ensure compatibility and appropriate educational apps and programmes to be easily installed. The school highly recommends the use of tablet devices including iPad or Android for Primary / Secondary students and Mac or Windows laptops for senior students.
- Phones are not used at school at any time, unless explicit permission has been given by the Principal. Students are able to use the phone after school. If students need to contact parents at any time this is allowed via the reception phone.
- Only One Device (BYOD) per user is allowed to be connected to school WiFi.

- Equipment problems should be immediately reported to a teacher / SLT / the IT engineer.
- It is prohibited to move, repair, reconfigure, modify or attach external devices to existing information and network equipment.
- All equipment must be properly signed-out/in and documented, and work areas kept neat and clean, free from food and drink.
- Users are expected to treat equipment with extreme care and caution; these are expensive devices that are entrusted to their care. Users should report any damage or loss to their Teacher / FL / Head of Year. If a person checks-out or borrows an equipment, they are responsible for replacing it or repairing it if it is lost or damaged. GFA will **not** be financially accountable for any loss or damage.

Violations

- Violations will result in a denial of access and possible further disciplinary action. Notification to parents, suspension of network, technology, or computer privileges, detention or suspension from school and school-related activities, legal action and/or prosecution
- Not respecting the values and ethics of the local host culture.
- Giving access of your password to any other user.
- Any attempts to transmit software designed to compromise the operation or security of the school network in any manner.
- Install and use of virtual Private networks within the school network and outside.
- Use school technologies to pursue information on illegal activities.
- Any attempts to circumvent the licensing control or the copying of software from the network.
- Students should not download or attempt to download any software on to school equipment.
- Use or attempt to use another student's assigned hardware, subscriptions, files, or personal information.
- Tampering or experimenting with the school network or equipment, including efforts to bypass the school's Internet filters or proxies.
- Use school technologies in a way that could be personally or physically harmful.
- Attempt to hack or access sites, servers, or content that isn't intended for my use.
- Use school technologies to send spam or chain mail.
- Plagiarise content I find online and attempt to find inappropriate images/content
- Post personally-identifying information, about myself or others
- Use language online that would be unacceptable in the classroom and/or at home

Mobile Device Monitoring

The school will use available MDM and block software to filter objectionable materials on the Internet in order to help ensure the safety of all students. Access to the Internet, including web sites, content, and online tools will be restricted in compliance with UAE regulations and GEMS policies. Web browsing may be monitored and web activity records may be retained indefinitely. Email usage, web posts, chats, sharing, and messaging may be monitored.

Netiquette

- Users should not attempt to open files or follow links from unknown or untrusted origin.
- Students are not to have WhatsApp connection with staff but are allowed only through registered email only.
- Recognising the benefits collaboration brings to education, GFA provides students with access to web sites or tools that allow communication, collaboration, sharing, and messaging among students. Students are expected to communicate with appropriate, safe, mindful, courteous conduct online as offline.
- Playing commercial/online games and visiting sites not related to education is not permitted. Watching DVDs, Movies, TV Shows, etc. while at school is prohibited
- Respect the use of copyrighted materials.
- Respect the rights and privacy of others.
- Installation of software and applications on students' own devices is permitted insofar as it does not conflict with the security requirements outlined above or the primary purpose of such devices as learning tools. Downloading of unauthorised programs is not allowed.

- Avoid modifying or copying any protected system files, system folders, or control panel files on school equipment.
- Obey the laws and restrictions of UAE, do not use personal equipment to record (audio/visual) of others without their permission and upload them.
- Alert a teacher or other staff member if you see threatening, appropriate, or harmful content (images, messages, posts) online and help maintain the integrity of the school network.
- Students should use trusted sources when conducting research via the Internet.

Cyber bullying/social media

Cyber bullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber stalking are all examples of cyber bullying. Students should not send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviours, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyber bullying can be a crime. Remember that your activities are monitored and retained.

Students will be held accountable for Cyber-bullying, even if it occurs off-campus during the school year and negatively impacts the academic environment at GFA. Students are reminded that in the UAE there are extreme consequences for online defamation of character of person or organisation.

The UAE Student Conduct Disciplinary Bylaw and the Federal Decree-Law no. (5) outline that deliberately creating, transferring and publishing photos and comments on Social Media (Instagram and WhatsApp) that undoubtedly shows defamation of individuals or staff members or School Leadership of character, dignity and integrity are breaking the law.

Key provisions relevant to schools' excerpts of Federal Decree-Law no. (5) state:

21	Invasion of privacy, including photographing others, or creating, transferring, disclosing, copying or saving electronic photos (just taking a photo or video of someone without their permission, or saving a photo they have posted, is enough). Defamation. Publishing news, photos, scenes, comments, statements or information, even if true and correct. Amending or processing a record, photo or scene for the purpose of defamation of or offending another person or for attacking or invading his privacy.	Up to 6 months' imprisonment +/ fine of AED 150k – 500k

Students need to be fully aware of their responsibilities that is reinforced at school via the curriculum that covers Common Sense Media. This provides the students with a clear understanding of the above conditions within the UAE and includes comprehensive coverage of issues relating to students' own 'digital footprints' and creating a positive online presence, as well as interaction with others.

Student, School and Parent Agreement

- I acknowledge that I am responsible for my actions on my device, in school, at home and elsewhere, and for following the specific rules established for the use of the hardware, software and networks throughout the school and beyond. I understand that failure to do so could result in a loss of technological privileges.
- I agree that I will not share my passwords or account details with anyone and will have full

- responsibility for the use of my account. I will not use another's account or represent myself as someone else.
- I agree that I will not engage in illegal activities on the school network or any other digital environment (e.g. plagiarism, bullying, harassment, tampering with hardware, software or documents, vandalism, unauthorised entry or destruction of files or deliberate introduction of computer viruses).
- I agree that I will obey procedural safeguards to maintain the performance of the school's network and digital devices.
- I agree that I will respect the rights of others, use appropriate language, and avoid offensive or inflammatory material. I will bring incidents of offensive or inflammatory material directed to myself or others to the attention of a GEMS Education staff member.
- I agree that I will not share, make, or post online, personally identifying information about any members of the GFA community without permission (addresses, phone numbers, email
- addresses, photos, videos, etc.).
- I agree that I will access only those resources that are appropriate for school and those resources for which I have specific authorization.
- I agree that I will obey copyright laws and license agreements. Text material, music, software, and other media are protected by law.
- I agree that I will not install software on the school's network or digital devices without permission of the system administrators.
- I agree that I understand that system administrators and teachers may access my files during system maintenance or as a directed action.
- I agree that students who are issued school devices are responsible for their care. Charges related to repair and replacement caused by abuse, misuse, negligence or loss as determined by school administration will be the responsibility of the student and his or her parents.

I acknowledge that my son/daughter and I have read the above and understood its content and I am fully competent to give my consent. And will instruct my child regarding the importance of following guidelines included in this Acceptable Use agreement. I have signed the summary document that show that I have read and accepted all content included.

Signed: _____ **Date: _____**