GEMS Cambridge International Private School Sharjah
E-Safety Policy

Last Amended: August 2023
Policy Review Date: August 2024

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, 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:

- GCS Behaviour Policy
- MoE Distance eLearning Behaviour Policy
- GCS Safeguarding and Child Protection Policy
- GEMS Acceptable Use Policy
- GCS Inclusion Policy
- GCS Anti-bullying Policy
- GCS Distance Leaning Policy
- GCS Teaching and Learning Policy
- GEMS Remote Learning and Safeguarding Policy
- GEMS Online Compliance Policies

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

Leadership

Roles and Responsibilities

(See Appendix A - E-Safety Terms of Reference)

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 E-Safety 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 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

E-Safety Officer:

- Leads the E-safety Team
- 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
- Reports regularly to Senior Leadership Team

Child Protection/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

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 SPEA / 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, 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
- 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
- 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.

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:

- 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 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
- The E-Safety Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

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 / SPEA / or another relevant organisation
- Participation in school training / information sessions for staff

Standards and Monitoring

Bring Your Own Device (BYOD)

(See GCS Acceptable Use and BYOD Policy – Appendix B)

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 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 SPEA 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 SPEA
- 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 E-safety team and 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 GCS 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

	Incident Description	**Action and Reporting**
1st Degree Offences	Not attending classes or being on time	Follow Behavoiur Policy – First Degree Offences. Record on Phoenix and on E-satefy Log
	Using the microphone feature, camera or chat without prior permission from the teacher. Playing games (except with the express permission of the teacher because it is an educational necessity linked to the lesson.) Misusing rights and tools available through Microsoft Teams/Phoenix Classroom.	
	Misuse of emojis in the chat	
	Unkind/ disrespectful comments towards the teacher or others	
	Not muting their microphones when asked to do so Failure to follow the rules of positive behaviour inside and outside the class, such as remaining calm and maintaining discipline during the period, and making inappropriate sounds inside and outside the class.	
2nd Degree Offences	Use of inappropriate language	Follow Behaviour Policy – Second Degree Offences. Record on Phoenix and on E-safety Log
	Absence from a single school day (via distance learning) without an acceptable excuse.	
	Misusing any means of communication.	
	Engaging in audio and video communication (MS Teams) with the rest of the students for non-educational purposes after the end of the official period time, be it on or off school premises.	
	Removing the teacher or students from the group that leads to blocking the course of the lesson, teacher’s work and other students' rights.	
	Using profanity, racial slurs, or other language (text, sound, or hint) that may be offensive to any other user. Abusing or insulting official visitors during periods during the live broadcast.	

	Verbal abuse or insulting students, staff or school guests.	
	Incitement to fight, threaten or intimidate classmates.	
Level 2 E-safety Addendum **The following steps are now place for any student in the school who are brought to our attention via Impero or any other communication channel due to inappropriate / unacceptable use of language on our computers**	1. *The IT Team informs the E- Safety team immediately (which includes the exec team) of any inappropriate use of language* 2. *The Head of School notifies the Senior Leader / Head of Year and Pastoral Lead for Secondary.* 3. *The Senior Leader / Head of Year or Pastoral Lead calls the parent on the same day of the offence and ask the parents to attend a meeting in person at school – ideally on the same day / as soon as possible the next day* 4. *The meeting is led by the Senior Leader / Head of Year and Pastoral Lead* 5. *It is made clear to the parent and the student that we have a zero tolerance of the use of inappropriate language – the parent / student / senior leader and Pastoral lead to sign the GCS Letter by the end of the meeting. –*	
3rd Degree Offences	Cyber bullying	Follow Behaviour Policy – Third Degree Offences. Record on Phoenix and on E-safety Log .
	Attempting to defame or abuse schoolmates and/or personnel on social media.	
	Racist language towards others	
	Divulging other students' personal information, including home addresses and phone numbers.	
	Searching for information, obtaining specific copies, or modifying files and other data, or passwords belonging to other users on the network. Entering and using the account of another teacher or student with or without his/her knowledge and/or consent.	
	Destroying, modifying, or misusing devices or software in any way. Tampering, removing, requesting the removal of, or intentionally causing damage to any device, software or hardware. Installing or downloading software or products that might harm the device or the network.	
	Using any camera (available as part of or as an add-on to certain devices) for personal use, and/or sharing photos or any information about any of the students' parents, employees, or any other person without their explicit consent. Using educational content to photograph and recording conversations between	

	students, and posting them without prior permission.	
	Forging school documents/impersonating others.	
	Photocopying, possessing, publishing and circulating images of school personnel and students without their permission.	
4th Degree Offences	Using any means of communication or social media for illegal or immoral purposes, or to harm an educational institution, its employees, or others.	Follow Behaviour Policy – Forth Degree Offences. Record on Phoenix and on E-safety Log .
	Publishing, creating, exchanging or promoting malicious or suspicious software.	
	Cheating in an official internal/external assessment.	

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 Phoenix H&E Portal 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 SPEA 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. The completed form should be retained by the group for evidence and reference 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

Appendix A

E-Safety Group Terms of Reference

A consultative group that represents our school/ community, we are responsible for:

- Blended Learning
- Digital Citizenship
- Online safety
- Monitoring the online safety policy including the impact of initiatives.
- This group will also take responsibility for reporting their findings to SLT and the Local Advisory Board (LAB)

Group Members

Core Team	
Charne Rossouw *Head of Primary*	DSL/E-safety Officer
Helen Mumford *Deputy DSL and Deputy Head of Secondary*	Safeguarding Officer
Keiron Tucker *Head of Secondary*	Safeguarding Officer
Shahana Salman *SLT – Whole School Community and Culture Lead*	E-Safety Inspector
Shellie Chaudhary *SLT – Whole School UAE Agenda and Design Thinking Lead*	Digital Citizenship and Design Thinking Officer
Muhammad Rafeeq *IT Engineer*	Information Asset Owner, Data protection and infrastructure Officer
Nora Said Rasha El Kattan *School Counsellors*	Welfare Officers
Extended Team	
Nitin Chaudhary *Technology & Marketing Specialist*	E-safety Mentor
Asif Mukadam	Parent Committee and LAB member/ Governor
Zara Khan	Executive Secretary and Parent representative
Design Thinking Student Leaders Digital Champions Student Leaders	Student Voice

Other people may be invited to attend the meetings at the request of the E-safety Officer or the behalf of the committee to provide advice and assistance where necessary.

Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature.

When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities.

Roles and Responsibilities

Function of the E-Safety Group

- To assist the E-safety Officer and DSL.
- To keep up to date with new developments in the area of online safety.
- To review and develop the online safety policy in line with new technologies and incidents. To monitor the delivery and impact of the online safety policy.
- To monitor the log of reported online safety incidents which to inform future areas of teaching / learning and training.
- Monitor incidents involving cyberbullying for staff and pupils.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. Information is disseminated out through:
    - Staff meetings
    - Student / pupil forums
    - Governors / LAB meetings
    - Surveys /questionnaires for students / pupils, parents / carers and staff
    - Parents' evenings
    - Website/VLE/Newsletters
    - Online safety events
    - Internet Safety Day

DSL and Child Protection Lead/E-safety Officer – Charne Rossouw

- Scheduling meetings and notifying committee members
- Inviting other people to attend meetings when required by the committee
- Guiding the meeting according to the agenda and time available
- Ensuring all discussion items end with a decision, action or definite outcome
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary
- Following the agreed procedures as set out within the Safeguarding and Child Protection Policy.
- Know how to identify the signs and symptoms of abuse.
- Providing advice and support to staff in matters of Child Protection.
- Report allegations and suspicions to the Principal.
- Maintaining accurate records of incident reports and any follow-up actions.
- Ensuring all records are kept confidentially, separate from the main student files in a locked location in the Head of School's office.
- Knowing when and how to make a referral to outside agencies and professionals.

Information Asset Owner, Data protection and infrastructure Officer

- Ensure that monitoring is carried out of Internet sites used across the school
- Monitor filtering / change control logs (e.g. requests for blocking / unblocking sites). Monitor the safe use of data across GCS.
- Keep up to date with SPEA / GEMS policies and protocols

Safeguarding Officers – Keiron Tucker and Helen Mumford

- Supporting the E-safety Officer and DSL in following the agreed procedures as set out within the E-Safety, Safeguarding and Child Protection Policy.

E-Safety Inspector – Shahana Salman

- Liaising with the GCS parent community to share school initiatives and gather feedback in order to improve e-safety at the school.
- Monitoring e-safety incidents
- Facilitating student leadership and student-led events
- Facilitating whole school initiatives

Design Thinking and Digital Citizenship Officer – Sheillie Chaudhary

- Facilitating student leadership and student-led events
- Facilitating whole school initiatives

Welfare Officers

- Support the E-safety team with any behaviour, counselling or safeguarding issues that might arise
- Raise awareness on the importance of Digital Citizenship and wellbeing within the GCS community

Standing Agenda Items

- Review and update of actions from last meeting
- Review of e-safety incidents – E-safety Officer and DSL and SLT
- New national guidance or policy requirements – E-safety Officer
- Filtering reports – IT Engineer
- IT security issues - IT Engineer
- Concerns or questions from the community – Parent committee member
- Any other business - including proposals for new initiatives

Other regular items may include

Anti-bullying week
Safer Internet Day
Annual review of e-safety incidents
Discuss appropriate training needs as required (staff, governors, parents)
Review e-safety curriculum, e-safety and acceptable use policies

Duration of Meetings

Meetings shall be held monthly for a period of 1 hour.
A special or extraordinary meeting may be called when and if deemed necessary.

Appendix B

GEMS Cambridge International Private School Sharjah Bring Your Own Device and Acceptable Use Policy

Last Amended: June 2023
Policy Review Date: June 2024

This document covers the use of BYOD and related technologies in the school: i.e. email, internet, intranet and network resources, learning platforms, software, equipment and systems. Digital systems, technologies and software are made available to students to further their education and to help the management of the school. This Acceptable Use Policy has been drawn up to protect students, staff and the school. The school reserves the right to examine or delete files that may be held on its computer systems and to monitor any Internet site visited or work done by a student.

At GCS we will do our best at integrating technology into our classes. This ensures our students are taught not only the fundamentals but real-life applications, flexibility and stay updated with our ever-changing technology.
However, for this system to be beneficial, our students must adhere to the policy:

Requirement 1- APPROPRIATE USE OF THE NETWORK RESOURCES

- Internet access is available to all students and staff at GCS. We believe
- these communication links offer vast, diverse and valuable resources to both students and staff.
- Students are expected to access only the school's WiFi network when on the premises.
- Students are expected to access only educational sites and applications when in school.
- All members of the GCS community will respect the values and ethics of the UAE. Users must not access or post inappropriate materials. This includes plagiarism, hate mail, cyberbullying, chain letters, unauthorised access (hacking), and email messages that initiate false alarms, etc.
- The school will use available monitoring and blocking software to filter search
- material on the Internet.
- Activities that degrade the performance of the network are strictly prohibited and will result in suspension of network privileges. For example, peer-to-peer file sharing, downloading software, video or audio files.
- The use of VPNs is prohibited.
- For Secondary students, email is allowed during school hours only in connection with a classroom assignment.

Requirement 2 – RESPECT AND MAINTAIN SCHOOL AND PERSONAL DATA/PROPERTY

- Student-owned technology used at school is expected to be in good working condition with only properly licensed software installed, and sufficient battery life to operate when required in classrooms.
- Faculty and staff may check laptops at any time to verify ownership.
- Software, hardware and peripherals are provided as tools for student use for educational purposes. Students are not permitted to install software, relocate

hardware (except for portable devices), install peripherals or modify settings to equipment without the consent of the technology department.

- Report equipment problems immediately to instructor / tech assistants / Network Administration / IT Engineer.
- Leave workstations and peripherals in their designated places.
- Keep work areas neat and clean and away from food and drink.
- Users should respect the rights of others using the school technology resources by: using assigned workstations, if required by the teacher; always logging off workstations; never attempting to disrupt network performance or interfering with the work of another user; and leaving equipment and room in good condition for the next user/class.
- The use of devices owned by the school is only permitted under teacher supervision in classrooms or designated computer zones.

Requirement 3 - RESPECT FOR OTHER USERS, INCLUDING PRIVACY AND PROPERTY

- Students will be held accountable for cyber-bullying or the passing of inappropriate/illegal content, even if it occurs off-campus during the school year and negatively impacts the academic environment at GCS.
- Students will promptly disclose to a teacher or other school employee any message received that is inappropriate or makes the student feel uncomfortable.
- Each user shall respect others' work, files, passwords and property (hardware and software).
- Users shall not misrepresent themselves, others or GCS in communications and/or online posts.

Requirement 4 - RESPECT FOR SECURITY

- Accounts on the systems at GCS are considered secure, although absolute security of any data cannot be guaranteed. Teachers can be provided access to student files for instructional or evaluative purposes.
- Use only their account/password (Note: It is a violation to give access to their password to any other user).
- Students must immediately notify a teacher or the system administrator if they have identified a possible security problem. Students should not go looking for security problems, this may be construed as an illegal attempt to gain access.
- Students will not attempt to gain unauthorised access to any portion of the GCS electronic network.
- Users will not attempt to access websites blocked by district policy, including the use of
- proxy services like VPN’s, software, or websites.
- Users will not use sniffing or remote access technology to monitor the network or other user’s activity.

Requirement 5 - EXPECT MONITORED USE

- Understand that communication systems and use of networks should not be considered confidential and may be monitored by the school at any time to ensure reliability, integrity, security and appropriate use. Files stored on the network are treated in the same manner as other school storage areas, such as lockers. Routine maintenance and monitoring of electronic network may lead to discovery that a student has violated this policy or the law. Students should not expect that files stored on district servers are private.

- Students' right to free speech applies to communication on the Internet. GCS's electronic network is considered a limited forum, similar to the newsletter and thus restrictions of speech should be expected for valid educational reasons.
- An individual search will be conducted if there is reasonable suspicion that a student has violated this policy or the law. The investigation will be reasonable and related to the suspected violation.es

Requirement 6 - PERSONAL EQUIPMENT

- All users must follow all policies even while using their own personal equipment.
- Watching movies, TV shows, etcetera while at school is prohibited.
- Private networks are prohibited within the school network.
- Playing commercial/online games or using applications not sanctioned by a teacher is not permitted.
- Accessing social media apps (E.g., WhatsApp/iMessenger) is prohibited.

CONSEQUENCES FOR VIOLATING ACCEPTABLE USE POLICY

Violations of this policy may result in loss of access as well as other disciplinary or legal action.
Student violation of this policy shall be subject to the consequences as indicated within this policy as
well as other appropriate discipline, which may include but is not limited to:

- Use of network only under direct supervision
- Suspension of network privileges
- Revocation of network privileges
- Suspension of computer privileges
- Suspension from school
- Expulsion from school and/or
- Legal action and prosecution by the authorities

The school administrators shall determine the particular consequences for violations of this policy. The Principal designee shall determine when school expulsion and/or legal action or actions by the authorities are the appropriate course of action.

INTERNET/WORLD WIDE WEB USAGE

The school will use available monitoring and blocking software to filter objectionable materials on the Internet. Internet access is available to all students and teachers at GCS. We believe these communication links offer vast, diverse and unique resources to both students and staff and their availability outweighs any possible access to information that is not consistent with the educational goals of GCS. However, both student and parent are asked to sign the school's Home School Agreement which includes an Acceptable Use Policy while their children attend GCS that will be enforced during the student's attendance at the school.

Expected standards of conduct include:

- I understand that I must use the school digital system in a responsible way, to ensure that there is no risk to my safety, other students or to the safety and security of the digital systems
- For my own personal safety:
- I understand that only tablets and laptops suitable for learning will be used in school, mobile phones will only be allowed for specific educational purposes, when asked.
- I will only use the school's WiFi network when on the premises.
- I will not use VPNs or other private networks while using devices at school.
- I understand that the school is not responsible or liable for loss or damage, or for maintenance or repair of my device.
- I understand that the school does not provide any insurance cover for personal devices brought to school.
- I understand that the school will monitor my use of digital systems, email and other digital communications. This will include monitoring and accessing any personal folder on my device.
- I understand that the school's digital systems are intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so. I will only use devices for schoolwork, homework and as directed.
- I will not bring files into the school (on removable media or online) without permission or upload inappropriate material to my institution.
- I will only edit or delete my own files and not view or change other people's files without their permission.
- I will ensure I have a secure password on my device and keep my logins, usernames and passwords undisclosed.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems for on-line shopping, on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting.
- I will use the Internet responsibly and will not visit web sites I know to be inappropriate for the school.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will immediately report any unpleasant, inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line to a teacher / trusted adult.
- I will not disclose or share personal information about myself or others when on-line.
- I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless I take a trusted adult with me.
- I am aware that some websites have age restrictions and I will respect this.
- I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
- I will not take or distribute images or videos of anyone without their permission. (This is an offense by UAE law)
- I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not install or attempt to install programmes of any type on a machine or store programmes on a computer. I will not alter computer settings.
- When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work. Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I understand that I am responsible for my actions, both in and out of the school.
- I understand that the school also has the right to act against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement even when I am out of the school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, removal of devices, contact with parents and in the event of illegal activities involvement of the appropriate authorities.

Name: ______________________________

Class: _____________________________

Signed: ____________________________

Date: ______________________________

Appendix C

Schedule for Development / Monitoring / Review

This e-safety policy was created in:	August 2023
The implementation of this e-safety policy will be monitored by the:	SLT and the E-Safety Team
Monitoring will take place at regular intervals:	Daily, Weekly, Termly, Annually
The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Annually
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	August 2024
Should serious e-safety incidents take place, the following external persons/agencies should be informed:	Albie Huyser (Principal/CEO) Charne Rossouw (DSL Lead/E-safety Officer) Helen Mumford (Deputy DSL)