GEMS Cambridge International Private School Sharjah E-Safety Policy

Last Amended: August 2020
Policy Review Date: August 2021

Schedule for Development / Monitoring / Review

This e-safety policy was created in:	January 2021
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 2021
Should serious e-safety incidents take place, the following external persons/agencies should be informed:	Albie Huyser (Principal/CEO) Charne Rossouw (E-safety Officer) Michellle Motley (DSL lead)

Scope of the Policy

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

- GCS behaviour Policy
- MoE Distance eLearning Behaviour Policy
- Safeguarding and Child Protection Policy
- Acceptable Use Policy
- Inclusion Policy
- Anti-bullying Policy
- Distance Leaning Policy
- 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.

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.

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 behaviors 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 eg 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:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body (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 / Safeguarding Designated Safeguarding Lead

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

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

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 realize that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Caregivers:

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

- Digital and video images taken at school events
- Access to parents' sections of the website / 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.

Acceptable Use of Technology

Infrastructure

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

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

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 & 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

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

- Attendance at training provided by the school / SPEA / or other 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 recognize 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 pupils 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 sex, 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.

Behaviour Incidents

	Incident Description	**Action and Reporting**
1st Degree Offences	Not attending classes or being on time	**Upon Committing Offence** 1st incident in one day: 1. Verbal recognition of the misbehaviour.

	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 Repetition on same day – 3 times – Level 2	2nd Incident per lesson: 1. Refer to Behaviour Ladder 2. Isolate the student from the group to work independently. 3. Provide a verbal reminder of proper conduct. **1st Repetition** Repeat steps 1 – 3 Record behaviour on Phoenix. Contact parents via email. **2nd Repetition** Repeat steps 1 – 3 Record behaviour on Phoenix. Call the parent/guardian. 1. Refer to Behaviour Ladder 2. Isolate the student from the group to work independently. 3. Provide a verbal reminder of proper conduct. **3rd Repetition** Teacher to notify Head of year/SLT member. Class Teacher/Form Tutor to open file on pupil (form **No. 6.**) Meeting with parents and issue a first written warning to the student with parent/guardian signature of acknowledgement. **Form No. 7.** Parents sign Ministerial Behaviour Policy **Record on Phoenix** **3rd Repetition on the same day – Level 2**
2nd Degree Offences	Use of inappropriate language Absence from a single school day (via distance learning) without an acceptable excuse. Using e-mail or social media to reveal information of a personal nature. 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	**Repeated First Degree Offences** Teacher and Year Group Leader to meet with parents. Issue Form **No. 9** to student and Form **No. 10** to parents. **Once Off Offences – Age-appropriate consequence** Class teacher to call the parent/guardian and issue a warning email for parent. Teacher to open file (Form No 6.). Student to attend a counselling session with school counsellor. **1st Repetition** Get the signatures of the parent/guardian and the student on a warning. Issue Form **No. 9** to student and Form **No. 10** to parents.

	periods during the live broadcast.	**2nd Repetition -Year Group Leader** Issue Form **No. 10** again. Issue student with Behaviour Report. Further counselling internecion. **3rd Repetition- SLT Member** Refer to School Counsellor/ pastoral leader /School Behaviour Management Committee to carry out a set of actions that would contribute to improving the student's behaviour. Create Individual Behaviour Plan.
3rd Degree Offences	Cyber bullying	**Repeated First Degree Offences surpassing the second degree.** Senior Leader to meet with parents. Issue Form **No. 9** to student and Form **No. 10** to parents. **Once Off Offences** Immediate convening of the School Behaviour Management Committee (Exec) to conclude a decision. An immediate summons of the parent/guardian and signing the decision **–** Form **No. 8** Senior Leader to meet with Parents and Issue Form **No. 7** *One day internal isolation.* **1st Repetition** Immediate convening of the School Behaviour Management Committee (Exec) to conclude a decision. An immediate summons of the parent/guardian and signing the decision **–** Form **No. 8** Head of Primary meet with Parents and Issue Form **No. 9** to student and **Form No. 10** to parents. *3-day internal isolation.* **2nd Repetition- Vice Principal to meet with parents and pupils** Issue a decision from the School Behaviour Management Committee to suspend the student. Xx days external suspension from school. **Issue Form No. 12** and seek support from Inclusion Team.
	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.	
4th Degree Offences	Publishing, creating, exchanging or promoting malicious or suspicious software.	Heads of School - Immediate communication with the parent/guardian.

	Cheating in an official internal/external assessment.	Take immediate procedure towards the offence with the help of the concerned parties. Suspend the student until the completion of the investigation. The student and his/her guardian shall be held responsible for any damages resulting from the offence. Transfer the student to the remedial programs approved by a decision of the school. Suspend the student's registration in schools and full denial of access to schools and the transition to continuous home schooling. Complete suspension in the case of exhausting all means of remedy.

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

It is hoped that 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 *Whole School Teaching and Learning Coach*	E-safety Officer
Michelle Motley	Safeguarding Officer

DSL and Head of Primary	
Walaa Elsayed *Deputy DSL and Head of MoE Subjects*	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 Desing Thinking Lead*	Digital Citizenship and Design Thinking Officer
Muhammad Rafeeq *IT Engineer*	Information Asset Owner, Data protection and infrastructure Officer
Asmaa Shehat *School Counsellor*	Welfare Officer
Fatma Abomahmod *School Counsellor*	Welfare Officer
Extended Team	
Nitin Chaudhary *Technology & Marketing Specialist*	E-safety Mentor
Asif Mukadam	Parent Committee and LAB member
Zara Khan	Executive Secretary and Parent representative
Desing 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

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

DSL and Child Protection Lead – Michelle Motley

- 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 Walaa Elsayed

- 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 – Asmaa Shehat ad Fatma Abomahmod

- 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.

Amendments

The terms of reference shall be reviewed annually from the date of approval.

They may be altered to meet the current needs of all committee members, by agreement of the majority.

The above Terms of Reference for GEMS Cambridge International Private School Sharjah have been agreed.

Date: January 2021
Date for review: August 2021