GCS E-Safety Policy – Summary Version for Parents











PURSUING EXCELLENC





GLOBAL CITIZENSHIP



GCS E-Safety Policy

Rationale and Purpose

The purpose and rationale of this policy is to keep all stakeholders informed of digital safety and what they need to do if they encounter a problem or need advice. As an education establishment it is our role to educate all stakeholders of today's digital world that we live in and to keep all our pupils safe online.

Policy Scope

- Links to other school Policies (Behaviour, Teaching and Learning, Curriculum, Inclusion, Acceptable Use, Home School Agreement, BYOD, Distance Learning Policies etc.)
- Roles and responsibilities
- GCS protocols and infrastructure
- Risks
- Education and Awareness
- Monitoring
- Reporting

























E-Safety and 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 of 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?

- 1. Content: What children and young people see online
- 2. Contact: Who they communicate with online
- 3. Conduct: How they act online

Online harmful behaviours:

- Online bullying and aggressive contact
- Access to inappropriate or illegal online content
- Meeting strangers online
- Exposure to inappropriate texts or images
- Self-harm
- Identity theft
- Over-engagement with technology e.g. gaming, social media, screen time
- Privacy
- Commercialisation and the impact of media on self-image and identity

(As published by EU Kids Online 2020)

























Policy and Leadership

Roles and Responsibilities

Governors-/ Local Advisory Board members - Are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Principal and Senior Leaders- The Principal and members of the Senior Leadership Team has a duty of care to ensure the safety (including e-safety) of all members of the school community

E-Safety Officer- Charne Rossouw- 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

Child Protection/Safeguarding Designated Safeguarding Lead-Michelle Motley, Walaa Elsayed & Keiron Tucker- Are trained in esafety and potential child protection / safeguarding issues

ICT Engineer/Technical staff- Muhammad Rafeeq-The ICT Engineer is responsible for ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack

Teaching and Support Staff- Are responsible for ensuring that they have up-to-date information of e-safety matters and of the current school e-safety policy and practices

Students- Are responsible for using the school digital technology systems in accordance to the Student Acceptable Use Policy

Parents / Caregivers- Play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way.

















LEADING THROUGH INNOVATION



EXCELLENCE



LEARNING



GLOBAL CITIZENSHIP



GCS E-Safety Core Team





Deputy DSL and Safeguarding Officer



Muhammad Rafeeq

Data Protection and Asset

Management Officer / IT Engineer



Welfare Officer and School Counsellor



Welfare Officer and School Counsellor



Shahana Salman

Cambridge

E-Safety Inspector



Sheillie Chaudhary

Design Thinking and Digital Safety Officer

















PURSUING EXCELLENCE





GLOBAL CITIZENSHIP



GCS Extended E-Safety Team



Nitin Chaudhary E-Safety Mentor



Nisha Rao Computing Teacher



Manju Joseph
Computing Teacher



Asif Mukadam

LAB Member and

Parent Committee Representative























PURSUING EXCELLENC





GLOBAL CITIZENSHIP



Infrastructure

How are we ensuring our network and school is safe?

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.

- Filtering and monitoring
- Network password security
- GEMS Reporting Procedures
- GCS Monitoring and Reporting Procedures
- GEMS/ GCS BYOD and Acceptable Use Policy
- Home School Agreement

























Education

Students

- Computing lessons
- Assemblies
- Safer Internet Days
- Class discussions
- Student leadership
- Posters and information

Teachers

Needs analysis surveys and staff training

Educating Parents

- Parent Webinars and workshops
- Parent surveys
- Newsletters
- Sharing resources
- School website and social media

Educating the Wider Community

- School website and social media
- Plasma TVs in school





















PURSUING EXCELLENC







Educating Students

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, home address, school they attend and parents' information (e.g. banking details).
- 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 ctizenship
- Cyberbullying
- Who to talk to/report to

























Educating Parents

Weekly Parent Webinars

GCS Newsletters

See Phoenix Classroom, School Community, Resources, Newsletters and Circulars

Informative Websites for Parents

Click on the images to access the links

































Educating Teachers

- Safeguarding, Behaviour Policy, E-Safety Policy Training (ladders, reporting and recording)
- E-safety Policy (ladders, reporting and recording)
- Information on where to access key policies
- GEMS Online Training
 - Information Security Awareness (Acceptable Use Policy, Information Security Awareness)
- E-safety Assemblies and student presentations
- Common Sense Media Training https://www.commonsense.org/education
- Support from SLT



















PURSUING EXCELLENC







Standards and Monitoring

The school provides opportunities for parents and students to receive information and / or education about online safety. The school runs meetings for parents and carers and has referenced online safety issues in communications (E.g. GCS newsletters, parent webinars, social media.)

The impact of our E-safety implementation is measured through:

- Our DLR report
- PASS survey results
- Ongoing discussions and communication with students, parents and teachers
- Stakeholder surveys
- Incident logs
- Counselling logs
- Online lessons

























Monitoring

Monitoring Online Lessons

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

SLT continuously do spot checks and follow the procedures in place if there are any suspected incidents of misuse.

Monitoring the School's Network

Our school network has a robust filtering and monitoring system in place which ensures that unwanted content (e.g. inappropriate language/social media) is blocked.

Monitoring Safeguarding Concerns

All safeguarding concerns are immediately reported to the DLS and monitored closely. Policies and procedures in place are strictly adhered to

Data Protection

See the GEMS GCS Acceptable Use Policy

Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Please see our Social Media Policy.





















PURSUING EXCELLENCE







Reporting

Responding to Incidents of Misuse - How are we reporting and dealing with incidents?

This guidance is intended for use when staff need to manage incidents that involve the use of online services. The E-safety Officer is briefed on all incidents.

Behaviour Incidents	
Level 1	Class teacher
Level 2	Class teacher, Heads of Year, SLT
Level 3	SLT, Heads of School
Level 4	Heads of School, Principal

Safeguarding Incidents
DSL - Michelle Motley (Head of Primary)
Deputy DSL – Wala Elsayed (Head of MoE subjects)
Keiron Tucker (Head of Secondary)

IT Incidents or Issues

Class teacher SLT

Heads of School

Helpdesk gcs@gemsedu.com

E-safety Concerns

Class teacher

SLT

Esafety gcs@gemsedu.com



















LEADING THROUGH INNOVATION



EXCELLENCE



LEARNING



GLOBAL CITIZENSHIP



E-Safety Behaviour Incidents and Consequences – Level 1

	Incident Description	Action and Reporting
1 st Degree Offences	Not attending classes or not being on time	Upon Committing Offence 1st incident in one day: 1. Verbal recognition of the misbehavior.
	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	2 nd 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.
	educational necessity linked to the lesson.) Misusing rights and tools available through Microsoft Teams/Phoenix Classroom.	1st Repetition Repeat steps 1 – 3 Record behaviour on Phoenix. Contact parents via email.
	Misuse of emojis in the chat	 2nd Repetition Repeat steps 1 – 3 Record behaviour on Phoenix.
	Unkind/ disrespectful comments towards the teacher or others	Call the parent/guardian. 1.Refer to Behaviour Ladder
	Not muting their microphones when asked to do so Repetition on same day – 3 times – Level 2	2.Isolate the student from the group to work independently. 3.Provide a verbal reminder of proper conduct. 3 rd Repetition Teacher to notify Head of year/SLT member. Class Teacher/Form Tutor to open file on pupil Meeting with parents and issue a first written warning to the student with parent/guardian signature of acknowledgement. Parents to sign Ministerial Behaviour Policy Record on Phoenix
		3 rd Repetition on the same day – Level 2





Cambridge International Private School SHARJAH

















LEADING THROUGH INNOVATION



PURSUING EXCELLENCE



GROWING BY



GLOBAL CITIZENSHIP



E-Safety Behaviour Incidents and Consequences – Level 2

	Incident Description	Action and Reporting
2 nd Degree Offences	Use of inappropriate language	Repeated First Degree Offences Teacher and Year Group Leader to meet with parents.
	Absence from a single school day (via distance learning) without an acceptable excuse.	Once Off Offences – Age-appropriate consequence Class teacher to call the parent/guardian and issue a warning email for parent. Teacher to open file.
	Using e-mail or social media to reveal information of a personal nature.	Student to attend a counselling session with school counsellor. 1st Repetition
	Removing the teacher or students from the group that leads to blocking the course of the lesson, teacher's work and other students' rights.	Get the signatures of the parent/guardian and the student on a warning. 2 nd Repetition -Year Group Leader Issue student with Behaviour Report.
	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.	Further counselling internecion. 3 rd 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.

















LEADING THROUGH INNOVATION



EXCELLENCE



GROWING BY



GLOBAL CITIZENSHIP



E-Safety Behaviour Incidents and Consequences – Level 3

summons of the One day internal isolation/exclusion from online learning. Summons of the One day internal isolation/exclusion from online learning. Summons of the One day internal isolation/exclusion from online learning. Counselling team intervention. 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		Incident Description	Action and Reporting
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	_	Cyber bullying	Repeated First Degree Offences surpassing the second degree.
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	Offences	Racist language towards others	Soniar Loador to most with parents
summons of the One day internal isolation/exclusion from online learning. Summons of the One day internal isolation/exclusion from online learning. Summons of the One day internal isolation/exclusion from online learning. Counselling team intervention. 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			
bestroying, 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		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	One day internal isolation/exclusion from online learning. Counselling team intervention. 1st Repetition
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		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	summons of the parent/guardian and signing the decision . 3-day internal isolation/ exclusion from online learning.
		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.	Issue a decision from the School Behaviour Management Committee to suspend the student. Xx days external suspension
Forging school documents/impersonating others.		Forging school documents/impersonating others.	





مدرسة جيمس كامبريدج إنترناشونال الخاصة بالشارقة Cambridge International Private School sharjah























E-Safety Behaviour Incidents and Consequences – Level 4

	Incident Description	Action and Reporting	
4 th Degree Offences	Publishing, creating, exchanging or promoting malicious or suspicious software.	Heads of School - Immediate communication with the parent/guardian. Take immediate procedure towards the offence with the help of the concerned parties.	
	Cheating in an official internal/external assessment.	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.	

*Note: Some incidents can be classified as safeguarding concerns and will be referred to the DSL – Designated Safeguarding Lead.

























Example Safeguarding Incidents

Incident Description	Action and Reporting
Sharing inappropriate or explicit images	1. Class teacher reports to DSL following the
Using Teams/Phoenix Classroom after hours / late in the evenings	safeguarding reporting procedure 2. DSL meets with parents, records it on
Sharing personal information	Phoenix Health / GEMS Safety Portal 3. DSL refer to school counsellors or GEMS
Sharing inappropriate photos of themselves	DSL lead where appropriate 4. Monitoring and follow up where appropriate
Inappropriate use of the camera during online lessons	



GCS DSL – Designated Safeguarding Lead: Michelle Motley (Head of Primary)

m.motley gcs@gemsedu.com

GCS Deputy DSL – Walaa Elsayed (Head of MoE Subjects)

w.elsayed gcs@gemsedu.com







مدرسة جيمس كامبريدج إنترناشونال الخاصة بالشارقة Cambridge International Private School SHARJAH

















INNOVATION



EXCELLENCE



LEARNING



GLOBAL CITIZENSHIP



Posters Shared with Students

Behave Smart and Stay Safe Online



SHARE

RESPONSIBLY

We all love to share photographs, fun things we're doing and much more.

Be careful what you share and always ask permission if somebody else is in the photo or video.



MANAGE

your PRIVACY

If you're using apps that can communicate with others, turn on privacy.

Only let people you really know follow you unless you've asked permission from your parents.



ASK

for HELP

Don't ever be worried about asking for help from someone you trust.

You will NOT be judged.



RESPECT

OTHERS

Be kind.

Other people mau have different opinions from you.

That's okay, but if they become abusive, take screenshots. block and report and tell an adult.



THINK

CRITICALLY

TRUST

your INSTINCT

Is it true? Does that person really know me? Has that really happened?

Alwaus question!



If anything worries you, or if you need help with something

speak to a trusted adult, your class teacher or form tutor











































INNOVATION

PURSUING EXCELLENCE





GLOBAL CITIZENSHIP



Anonymous Reporting Facility for Students





مدرسة جيمس كامبريدج إنترناشونال الخاصة بالشارقة Cambridge International Private School











