جيمس مدرستنا الهندية
GEMS OUR OWN INDIAN SCHOOL
Anchored In Excellence

E-SAFETY POLICY

Approved by:	Mrs. Prathima Nag A	**Date:** 25-05-23
Last reviewed on:	25-05-23	
Next review due by:	20-05-25	

Table of Contents

1. Introduction

Our school community recognizes the importance of treating e-safety as an ever-present serious safeguarding issue. It is important to protect and educate both Students and staff and have supportive mechanisms, policies and protocols in place to protect and support the school community. The safeguarding aspects of e-safety are evident in all our ICT/safeguarding policies and procedures throughout the school and it is essential that this constantly developing area of technology is kept under review. This policy links all the ICT, safeguarding and other policies and procedures to reflect how the school deals with e-safety issues on a daily basis.

2. Objectives and targets

This policy is aimed at making the use of electronic communication at GEMS Our Own Indian School, as safe as possible. This policy applies to all members of the school community (including staff, Students, volunteers, parents/guardians, visitors, community users) who have access to, and are users of, school ICT systems, both in and out of school.

3. Action plan

The school will deal with any e-safety incidents which may arise by invoking this policy, & other related policies. The school will inform parents of incidents of inappropriate e-safety behavior that take place in & out of school and will take appropriate action.

The Following sections outline:

- The roles and responsibilities for e-safety of individuals and groups within the school, and how they will receive education/training to fulfil those roles.
- How the infrastructure is managed.
- How e-safety is considered in the curriculum.
- The protocols on using digital images.
- The protocols on data protection.
- The protocols for handling electronic communication.
- Awareness of and dealing with inappropriate use of electronic media.

4. Roles and responsibilities

Principal

- Principal are responsible for reviewing the effectiveness of the policy.
- A nominated link Principal for e-safety is appointed.

- Principal receive e-safety training/awareness sessions as part of their regular cycle of meetings.

4.1 Senior Leadership Team

- SLT is responsible for reviewing the effectiveness of the policy.
- SLT is responsible for ensuring the e-safety of members of the school community.
- The Principal and another member of the senior leadership team/e-safety coordinator will be aware of the procedures to be followed in the event of a serious e-safety allegation being made against any student or staff, including the Principal.
- The Principal has the authority to regulate the behavior of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behavior. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, even though they may take place out of school, but are linked to membership of the school.

4.2 E Safety coordinator

- Leads the e-safety committee.
- Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy and other related policies.
- Ensures that all members of 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 SLT and Principal for e-safety.
- Liaises with school ICT technical staff.

4.3 ICT Engineer

That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.

- That the school meets the e-safety technical requirements outlined in the relevant GEMS ICT acceptable usage and guidance.
- Users may only access the school's networks through a properly enforced password protection policy.

4.4 Teaching and Support staff

Teaching and support colleagues are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of the current school e-safety policy.

- They have read, understood and signed the relevant staff acceptable usage agreement, and have read other related policies e.g. mobile phone and social media policies.
- They report any suspected misuse or problem to the e-safety coordinator/Principal/senior leader/ICT coordinator/class teacher for investigation/action.
- Digital communications with Students (email/virtual learning environment (VLE)/voice) should be on a professional level and only carried out using official school systems.
- Students understand and follow the school e-safety policy and the pupil acceptable computer usage policy.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons, extracurricular and extended school activities.
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
- They are aware of the e-safety issues pertaining to email and social media usage.
- In lessons where internet use is pre-planned, Students 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.
- All staff receive e-safety training and understand their responsibilities, as outlined in this policy.

4.5 Child Safeguarding Officer.

The designated person for child protection/child protection officer is trained in e-safety issues and will be aware of the potential for serious child protection 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.

4.6 E-safety group

Members of the e-safety group (Principal, SLT member, staff member, student member, parent representative and ICT Engineer) will assist with the development of e-safety education.

4.7 Students

Students are responsible for using the school ICT systems in accordance with the Student acceptable usage policy and agreement, which they will be expected to sign before being given access to school systems.

- 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 school policies on the use of mobile phones, digital cameras and hand-held devices.
- Will be expected to know and understand school policies on the taking/use of images and on cyber-bullying.
- Will develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Will 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.

While 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. E-safety education will be provided in the following ways:

- A planned e-safety program will be provided as part of ICT lessons – this will include both the use of ICT and new technologies in school and outside school.
- Key e-safety messages will be reinforced as part of a planned program of assemblies and tutorial.
- Students will 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 will be helped to understand the need for the student acceptable computer usage agreement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Students will be taught to acknowledge the source of any information used and to respect copyright when using material accessed on the internet.
- Rules for use of ICT systems/internet will be posted in all relevant rooms and displayed on log-on screens.

4.8 Parents/Guardians

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

- Parents and guardians will be responsible for endorsing (by signature) the pupil acceptable computer usage agreement.

Research shows that many parents and guardians do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through Orientations / Newsletters / Emails / VLE.

5. Training:

- A planned program of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff will receive e-safety training as part of their induction program, ensuring that they fully understand the school e-safety policy and acceptable usage policies.

6. Management of infrastructure

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. The school will also ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the acceptable computer usage policy and any relevant e-safety policy and guidance.
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling will be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Engineer and will be reviewed, at least annually, by the e-safety committee.
- All users will be provided with a username and password by the ICT Engineer.
- Users are made responsible for the security of their username and password, must not allow other users to access the systems using their log in details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service.
- Any filtering issues should be reported immediately to the ICT Engineer.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the acceptable computer usage policy.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

- An agreement is signed by members of staff in possession of school provided laptops regarding the extent of personal use that users (staff/Students/community users) and their family members are allowed on laptops and other portable devices that may be used out of school.
- The school infrastructure and individual workstations are protected by up-to-date virus software.
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. All Staff are to adhere to GEMS data protection policy.

7. Curriculum

E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages in the use of ICT across the curriculum

In lessons where internet use is pre-planned, Students are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where Students are allowed to search the internet freely, eg using search engines, staff are vigilant in monitoring the content of the websites the Students visit.
- It is accepted that from time-to-time, for good educational reasons, Students may need to research topics (eg racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Engineer temporarily removes those sites from the filtered list for the period of study. Any request to do so will be recorded, with clear reasons for the need.
- Students are taught in all lessons to be critically aware of the content they access online and are 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.
- Using digital and video images
- When using digital images, staff inform and educate Students about the risks associated with taking, using, sharing, publishing and distributing images. In particular, they recognize the risks attached to publishing their own images on the internet eg on social networking sites.
- Staff 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.
- Any images should only be taken on school equipment. Personal equipment of staff should not be used for such purposes.
- 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. Written permission from parents or guardians will be obtained.

8. Data Handling

All data related to students will 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.

Staff will ensure that they comply with the secure data handling by:

- Taking care at all times to ensure the safe keeping of personal data, minimizing the risk of its loss or misuse.
- Using personal data only on secure password protected computers and other devices, and ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data.
- Transferring data using encryption and secure password protected devices.

9. Communication Technologies

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 will be expected to know and understand school policies on email, social media (and other relevant electronic devices protocols.)
- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Users must not respond to any such email but must follow the procedures in the email policy.
- Any digital communication between staff and Students or parents/guardians (email, chat, VLE etc.) must be professional in tone and content.

10. Unsuitable/Inappropriate Activities

Certain activities are referred to in the acceptable computer usage agreements as being inappropriate in a school context and users must not engage in these activities in school or outside school when using school equipment or systems. The school policies on child protection and safeguarding and e-safety must be followed if any

apparent, suspected or actual misuse appears to involve illegal or inappropriate activity eg:

- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.

Should any serious e-safety incidents take place, the appropriate external authorities will be informed

11. Monitoring and Reviewing

The school will monitor the impact of the policy using:

- Logs of reported incidents.
- Monitoring logs of internet activity (ie ISP, school network or managed service as appropriate).
- Internal monitoring data for network activity.
- Surveys/questionnaires of Students, parents and staff.

The policy will be reviewed by the SLT annually, or more regularly, in the light of any incidents that have taken place, significant new developments in the use of the technologies, or perceived new threats to e-safety as advised by the e-safety committee or others. The policy will be updated if any such changes are implemented during the year.

***