"ഭരണഭാഷ- മാതൃഭാഷ"

കേരള സർക്കാർ

സംഗ്രഹം

പൊതുവിദ്യാഭ്യാസ വകുപ്പ് - കേരളത്തിലെ പൊതുവിദ്യാലയങ്ങൾക്കുള്ള കൈറ്റ് പുറപ്പെടുവിച്ച സൈബർ സുരക്ഷാ പ്രോട്ടോകോൾ 2026 - നടപ്പിലാക്കുന്നത് സംബന്ധിച്ച് - നിർദ്ദേശങ്ങൾ നൽകി ഉത്തരവ് പുറപ്പെടുവിക്കുന്നു.

പൊതു വിദ്യാഭ്യാസ(ഡി) വകുപ്പ്

സ.ഉ.(സാധാ) നം.2978/2026/GEDN തീയതി,തിരുവനന്തപുരം, 30-04-2026

പരാമർശം:-
1. 23.02.2019 ലെ KITE/2019/1605(2) നമ്പർ സൈബർ സേഫ്റ്റി പ്രോട്ടോകോൾ
2. 27.09.2019 ലെ സ.ഉ(സാധാ) നം. 3847/2019/പൊ.വി.വ
3. 30.01.2023 ലെ സ.ഉ(സാധാ)നം. 818/2023/പൊ.വി.വ
4. 07.03.2026-ലെ കൈറ്റ് /2026/1605(1) നമ്പർ സർക്കുലർ
5. 21.04.2026 ലെ കൈറ്റ് /2026/1605(2) നമ്പർ കത്ത്

ഉത്തരവ്

പരാമർശം (1) ഉത്തരവ് പ്രകാരം സ്കൂൾ കുട്ടികൾക്ക് വേണ്ടി കൈറ്റ് സൈബർ സുരക്ഷാ പ്രോട്ടോകോൾ പുറപ്പെടുവിച്ചിരുന്നു. പരാമർശം (2) പ്രകാരം സ്കൂളുകൾക്കായി പുറപ്പെടുവിച്ചിരിക്കുന്ന സൈബർ സേഫ്റ്റി പ്രോട്ടോകോൾ കൃത്യമായി പാലിക്കേണ്ടതാണ് എന്ന് നിഷ്കർഷിച്ചുകൊണ്ട് സർക്കാർ ഉത്തരവും പുറപ്പെടുവിച്ചിരുന്നു.

2. 2019-ലെ സൈബർ സേഫ്റ്റി പ്രോട്ടോകോൾ പുതുക്കുന്നതിന് ഡയറക്ടർ ബോർഡ് യോഗങ്ങളുടെ തീരുമാനപ്രകാരം പൊതുവിദ്യാഭ്യാസ വകുപ്പ് പ്രിൻസിപ്പൽ സെക്രട്ടറി ചെയർപേഴ്സൺ ആയിട്ടുള്ള കൈറ്റ് ഡയറക്ടർ ബോർഡ് കൈറ്റിനോട് ആവശ്യപ്പെട്ടിരുന്നു. ഐടി വകുപ്പ് പ്രതിനിധി ഉൾപ്പെടെ അംഗങ്ങളായ, പൊതുവിദ്യാഭ്യാസ വകുപ്പിലെ ഐ.ടി സാങ്കേതിക സമിതി യോഗത്തിൽ ഇപ്രകാരം ഭേദഗതി ചെയ്ത സൈബർ സേഫ്റ്റി പ്രോട്ടോകോളിന് അംഗീകാരം നൽകുകയും അതിനനുസരിച്ച് കൈറ്റ് കേരളത്തിലെ പൊതുവിദ്യാലയങ്ങൾക്കുള്ള ഭേദഗതി ചെയ്ത സൈബർ സുരക്ഷാ പ്രോട്ടോകോൾ 2026 പുറപ്പെടുവിക്കുകയും ചെയ്തിട്ടുണ്ട്.

പ്രസ്തുത സുരക്ഷാ പ്രോട്ടോകോൾ 2026 ലെ നിർദേശങ്ങൾ അംഗീകരിച്ചു ഉത്തരവ് പുറപ്പെടുവിക്കണമെന്നു പരാമർശം (5) പ്രകാരം KITE CEO അഭ്യർത്ഥിച്ചിരുന്നു.

3. സർക്കാർ ഇക്കാര്യം വിശദമായി പരിശോദിച്ചു .കൈറ്റ് സൈബർ സുരക്ഷാ പ്രോട്ടോകോൾ 2026 നടപ്പിലാക്കുന്നത് സംബന്ധിച്ച് താഴെപറയുന്ന നിർദ്ദേശങ്ങൾ നൽകി ഉത്തരവ് പുറപ്പെടുവിക്കുന്നു.

1. പൊതുവിദ്യാലയങ്ങൾക്കുള്ള സൈബർ സേഫ്റ്റി പ്രോട്ടോകോൾ 2026 കർശനമായി നടലാക്കാൻ സ്ഥാപന മേധാവികൾ ആവശ്യമായ സംവിധാനങ്ങൾ (സ്കൂൾ സൈബർ സുരക്ഷാ കമ്മിറ്റി രൂപികരണം ഉൾപ്പെടെ) ഏർപ്പെടുത്തേണ്ടതാണ്.

2. പ്രോട്ടോകോളിൽ വിശദമാക്കിയിട്ടുള്ള വിവിധ തലങ്ങളിൽ ശ്രദ്ധിക്കേണ്ട കാര്യങ്ങൾ (സ്ഥാപന മേധാവികൾ, അധ്യാപകർ, വിദ്യാർത്ഥികൾ, രക്ഷിതാക്കൾ) കൃത്യമായി ആ വിഭാഗങ്ങളിലേക്കെത്താൻ ആവശ്യമായ പരിശീലനം എല്ലാ സ്കൂളുകളിലും ലിറ്റിൽ കൈറ്റ്സ് യൂണിറ്റുകൾ വഴിയും മറ്റു സംധിധാനങ്ങൾ ഏർപ്പെടുത്തിയും നൽകേണ്ടതാണ്.

3. സൈബർ സുരക്ഷാ പ്രോട്ടോകോൾ 2026 കൃത്യമായി പാലിക്കുന്നുണ്ടെന്ന് ഉറപ്പാക്കാനും അവയുടെ പുരോഗതി വിലയിലയിരുത്താനും എല്ലാ വിദ്യാഭ്യാസ ഓഫീസർമാർക്കും പൊതുവിദ്യാഭ്യാസ ഡയറക്ടർ നിർദ്ദേശം നൽകേണ്ടതും ആയത് സ്ഥിരമായി മോണിറ്റർ ചെയ്യേണ്ടതുമാണ്.

4. സൈബർ സുരക്ഷാ പ്രോട്ടോകോൾ കർശനമായി നടപ്പാക്കാൻ ആവശ്യമായ ഡിജിറ്റൽ സംവിധാനങ്ങൾ, വിവിധ പരിശീലനങ്ങൾ, മോണിറ്ററിംഗ് തുടങ്ങിയവ (കൈറ്റ് വിക്ടേഴ്സ് ചാനൽ, ലിറ്റിൽ കൈറ്റ്സ് ക്ലബുകൾ തുടങ്ങിയവ ഉൾപ്പെടെ പ്രയോജനപ്പെടുത്തി ക്കൊണ്ട്) കൈറ്റ് ഏർപ്പെടുത്തേണ്ടതാണ്.

(ഗവർണറുടെ ഉത്തരവിൻ പ്രകാരം)
എ പി എം മുഹമ്മദ് ഹനീഷ്
അഡീഷണൽ ചീഫ് സെക്രട്ടറി

പൊതു വിദ്യാഭ്യാസ ഡയറക്ടർ, തിരുവനന്തപുരം
ചീഫ് എക്സിക്യൂട്ടീവ് ഓഫീസർ ,കൈറ്റ്.
അക്കൗണ്ടന്റ് ജനറൽ(ഓഡിറ്റ്), കേരള, തിരുവനന്തപുരം
പ്രിൻസിപ്പൽ അക്കൗണ്ടന്റ് ജനറൽ(എ&ഇ), കേരള, തിരുവനന്തപുരം
കരുതൽ ഫയൽ/ഓഫീസ് കോപ്പി

ഉത്തരവിൻ പ്രകാരം

സെക്ഷൻ ഓഫീസർ

CYBER SAFETY PROTOCOL 2026

for School Children

AI Generated Image

പൊതുവിദ്യാഭ്യാസവകുപ്പ്
കേരള സർക്കാർ

KERALA INFRASTRUCTURE AND TECHNOLOGY FOR EDUCATION

KERALA INFRASTRUCTURE & TECHNOLOGY FOR EDUCATION (KITE)
Poojappura, Thiruvananthapuram - 695012
www.kite.kerala.gov.in, contact@kite.kerala.gov.in
Phone : 0471 2529800

Circular No.KITE/2026/1065 (1) Dated 07/03/2026

Government of Kerala

KERALA INFRASTRUCTURE AND TECHNOLOGY FOR EDUCATION

No. KITE/2026/1605(1)

Date: 07.03.2026

CYBER SAFETY PROTOCOL FOR SCHOOL CHILDREN

Sub:KITE – Issuance of the Revised Cyber Safety Protocol 2026 for public schools in Kerala – Reg.

Ref:1. Cyber Safety Protocol for public schools published by KITE vide Circular No.KITE/2019/1605(2) dated 23.02.2019.

2. ICT guidelines for schools issued vide G.O.(Rt) No. 818/2023/GEDN dated 30.01.2023.

3. Minutes of 22nd & 32nd Director Board meetings of the KITE held on 13.04.2023 & 02.02.2026.

4. Minutes of the meeting of the IT Technical Committee of Department of General Education, held on 06.03.2026.

In accordance with the recommendations of the Committee on the Welfare of Women, Children and the Physically Handicapped of the 13th Kerala Legislative Assembly, KITE issued the Cyber Safety Protocol for school children as per reference 1st cited. Furthermore, Government had introduced updated ICT guidelines for schools and educational offices, vide reference 2nd cited, explicitly mandating strict adherence to the Cyber Safety Protocol issued for schools. The Director Board of KITE has authorized KITE to revise and republish the Cyber Safety Protocol vide reference 4th cited.

As part of the curriculum revision initiated in 2024, Cyber Security has been included with high priority in both the revised ICT textbooks and Little KITEs training programs. KITE has prepared the draft of the new Cyber Safety Protocol for schools, after a detailed analysis of international models, research in the field, and national legislation. This draft has been formally approved by the Government constituted IT Technical Committee as per reference 4th cited.

In this context, the Cyber Safety Protocol for schools in Kerala, as cited in reference 1st cited, is hereby amended, and the **Revised Cyber Safety Protocol 2026** is published herewith. KITE shall establish the necessary mechanisms to update the protocol periodically and ensure the implementation of these guidelines.

K. ANVAR SADATH
Chief Executive Officer

CONTENTS

Cyber Safety Protocol

1. Introduction

In the present era, where the digital world has become an integral part of everyday life, awareness of the safety standards to be followed while using the internet and digital systems is of great importance. Children increasingly use modern technological devices not only as part of their learning activities but also for entertainment and communication.

While these technological advancements create new opportunities and innovative methods of learning, they also give rise to significant challenges. In a context where modern technologies, including Artificial Intelligence (AI), are being widely adopted in the field of education, it is essential to ensure their responsible and safe use alongside their benefits. In this regard, it is necessary to comprehensively address the risks associated with various dimensions such as digital content (Content), interactions involving digital content (Contact), behaviour in the cyber environment (Conduct), and digital agreements or transactions (Contract).

The school community, comprising students, parents, teachers, and non-teaching staff, while utilizing digital technologies, may be exposed to various forms of exploitation. These include, but are not limited to: AI Grooming, Deepfake Blackmailing, Voice Cloning, Online Luring, Cyberbullying, and the creation of Harmful Content. Furthermore, there are concerns that excessive use of digital devices may adversely affect the physical health, imaginative capacity, social behaviour, learning patterns, and mental well-being of children.

With the increasing spread of emerging technologies, it is important to avoid situations where unnecessary fear is created and their use is discouraged, rather than addressing the challenges that may arise from them. In the education sector, proactive interventions to ensure cyber safety are being implemented at multiple levels by Kerala Infrastructure and Technology for Education (hereafter KITE). Extensive initiatives have already been implemented to help students identify cyber threats, prevent cybercrimes, and address such related challenges. These initiatives are carried out through various platforms and programmes, including ICT textbooks for Classes 1 to 10, the Samagra Plus portal for providing digital content and supporting academic monitoring, the Little KITEs club—the largest IT student network in India—and KITE VICTERS, India's first fully integrated educational television channel.

The establishment of Cyber Safety Clinics in schools is one of the key initiatives undertaken as part of these efforts. KITE provides practical training on cyber safety to students, teachers, and parents through these clinics.

Such training programmes are planned and implemented with clearly designed training modules and centrally developed resources, supported by systematic monitoring. For this purpose, KITE also utilizes the expertise and support of institutions and individuals with proven competence and credibility at both national and international levels.

In a context where Artificial Intelligence (AI) technologies are becoming increasingly integrated into various devices, including smartphones and other gadgets, there is a possibility that, just as the digital divide has led to the marginalization and exploitation of individuals, an emerging AI divide may also expose people to similar risks. Recognizing this challenge,

KITE has designed and implemented initiatives to ensure that students and parents in Kerala are supported in overcoming such limitations. As part of these efforts, KITE provides direct training to teachers and students on AI, while also empowering members of the Little KITEs to act as trainers in delivering AI awareness and training programmes for parents.

To incorporate the rapid advancements in technology into the educational process, KITE provides expert training at regular intervals to Little KITEs members, KITE mentors, School IT Coordinators, and educational officers. Precautionary measures to be adopted during emergency situations in the cyber environment, as well as practical strategies to address emerging challenges, form important components of these training programmes.

Since the introduction of ICT education in schools across the state, guidelines and training on the effective and safe use of computers, related devices, and the internet have been provided at various levels. Some of the key measures are listed below.

- The lessons pertaining to cybersecurity incorporated into the Information and Communication Technology (ICT) textbooks prepared by the Department of General Education.
- Government Order No. 818/2023/GEDN dated 30.01.2023, issued by the General Education Department, containing guidelines for schools and educational offices.
- Government Order G.O. (Rt) No. 165/2018/G.Edn dated 10.01.2018, issued for enabling the effective utilization of the equipment, facilities, and services provided for transforming classrooms into hi-tech learning environments under the Hi-Tech School Project implemented as part of the Public Education Protection Mission, and the Memorandum of Understanding (MoU) signed between KITE and schools in accordance with this order.
- The module titled 'Amma Ariyan' (Let Mothers Know), prepared for imparting cybersecurity training to 4 lakh (400,000) parents through Little KITEs clubs.

2. Cyber Safety Protocol – Objectives

1. Ensure that children are provided with a Safe Digital Learning Environment under the responsibility and supervision of teachers and parents.
2. Create awareness that cyber security is not the responsibility of a single section alone, but a collective responsibility of the entire school system.
3. Enable students, teachers, institutional heads, and parents to effectively prevent cyber abuses (such as stalking, harassment, etc.) against children and others, and to seek appropriate legal remedies.
4. Enable children to identify and avoid online content (Content Risk) that is inappropriate for their age and developmental stage.
5. Create awareness among children and parents about online exploitation (Contact Risk) such as AI grooming, deepfake blackmailing, vishing (voice cloning), hacking, and identity theft, and thereby prevent online abuse against children.
6. Along with digital freedom, cultivate a robust cyber culture in children by instilling digital etiquette (Netiquette) — including what to view, what to share, what to avoid, and how to safely interact in the online world (Conduct Risk).

7. Create awareness regarding the protection of individuals' personal information (such as name, address, photo, phone number, account details, etc.) in online spaces from misuse by others.
8. Equip children to approach digital information with critical thinking, verify its authenticity, and thereby identify fake news and misinformation.
9. Create awareness regarding the risks of sharing personal or official confidential information while using Generative AI tools.
10. Create awareness among all stakeholders about relevant legislation, including the IT Act (2000), the Digital Personal Data Protection (DPDP) Act, 2023, and the IT Rules (Amendment 2006), which aim to prevent and regulate cybercrimes. Simultaneously, build the capacity of individuals to seek legal protection against cyber attacks and the misuse of Artificial Intelligence (AI).
11. Raise awareness among teachers, students, and the general public about the benefits of Free and Open-Source Software (FOSS) and its wide-ranging potential.
12. Promote the use of safe, cost-effective, and educationally adaptable free software in academic settings, thereby fostering digital autonomy.
13. Develop children as responsible digital citizens, capable of adhering to digital laws and providing leadership during cyber emergencies.

3. Cyber Security in the ICT Textbooks

Content related to cyber security has been included in both primary and secondary level textbooks. This inclusion has been made in accordance with the provisions outlined in the curriculum framework. Some of the key points incorporated in the textbooks are provided below.

1. The Class V ICT textbook chapter titled "Searching the Internet" introduces students to handling fake news and emphasizes the need to manage screen time effectively.
2. The Class VII ICT textbook chapter titled "Let's Search and Find" covers copyright, the influence of the internet in daily life, how artificial intelligence affects our internet usage, and correct engagement in the cyber world.
3. The Class VIII ICT textbook chapter titled "Internet: A Boundless Realm of Knowledge" elaborates on copyright, Creative Commons licenses, fair use of digital content, and safe internet practices.
4. The Class IX ICT textbook chapter titled "The Web of Goodness" explains the careful use of social media, securing login credentials and passwords, cybercrimes, the importance of fact-checking, and safe internet usage.
5. The Class X ICT textbook chapter titled "Cyber Space" discusses proper use of information in cyberspace, plagiarism, spoiler alerts, distinguishing right from wrong in the digital world, authentic sources of information, cyber etiquette, and the risks associated with excessive use of digital gadgets.

4. Government Order on ICT guidelines

The Government has issued the following guidelines (primarily related to cyber security) under the Government Order dated 30.01.2023 regarding the use of ICT capabilities in the field of education.

1. Digital content, digital libraries, and other academic resources may be provided to schools only after joint approval by SCERT and KITE. Proprietary software or software subject to licensing terms must not be deployed in schools under any circumstances.
2. The Cyber Safety Protocol issued for schools must be strictly followed. Activities such as hosting students' personal information on private servers, or sharing such data, must not be undertaken at the school level. E-governance applications not approved by the General Education Department, as well as specialized IT initiatives, may be implemented only after obtaining specific permission from the Department.

5. Scope and Beneficiaries of the Protocol

In this era of rapid technological expansion, particularly with the increasing prevalence of new types of fraud involving Artificial Intelligence (AI), this protocol serves to secure all digital interactions associated with schools. It incorporates legal safety standards in accordance with the IT Act (2000), the Digital Personal Data Protection (DPDP) Act (2023), and the IT Rules (Amendment 2026). Along with ensuring the security of digital devices and networks installed in schools as part of the Public Education Protection Mission and related initiatives in Kerala, this protocol is intended to benefit the following categories of stakeholders and areas.

1. Target Group

1. Children: All students from primary to higher secondary levels.
2. Parents: To monitor children's online activities and provide them with a protective digital environment.
3. Teachers and non-teaching staff: To ensure the safe use of digital systems in teaching activities and administrative functions.

2. Applicable Areas

1. Academic Activities: Digital classrooms, digital content, QR codes in textbooks, online training sessions, examinations, and similar activities.
2. Use of Artificial Intelligence: Employing AI tools for learning and training purposes.
3. Administrative Data Management: Handling personal information and academic records of students and teachers collected through portals such as Sampoorna, Sahitham, and Samagra Plus.
4. Network and IT Systems: Internet connections in schools, including K-FON, as well as laptops and computers.
5. School Financial Transactions: Collection of students' Aadhaar and bank account details for scholarships, uniform allowances, and conducting online financial transactions.
6. Student-Teacher Communication: Use of messaging groups (such as WhatsApp), email,

Learning Management Systems (LMS), and official platforms.

7. Social Media Use: Awareness of precautions when sharing personal photos and locations, and reporting cyber attacks.
8. Online Learning Environment: Use of the internet and digital devices by students both inside and outside school, along with management of screen time.
9. Student Training: Providing practical training to all students through Little KITEs IT Clubs and other initiatives.

For the implementation of the Cyber Safety Protocol in schools, students, teachers, and parents must all make a concerted effort. The key responsibilities for each stakeholder are outlined below.

6. Safeguards to be Ensured by the Head of the Institution

1. As per Government Order (Rt.) No. 165/2018/G.Edn. dated 10.01.2018 and Government Order (Rt.) No. 2177/2019/G.Edn. dated 06.06.2019, and in accordance with the special Memorandum of Understanding signed between the schools and KITE, it is the responsibility of the Head of the Institution to ensure that the internet facility provided in the schools is made available to all students without interruption during school working hours for educational purposes.
2. The use of Internet by the students must be under the supervision of teachers. Seating arrangements in places and labs where internet access is provided should be organised accordingly.
3. Provide strong and secure passwords for the Wi-Fi network of the school and arrange a Guest Wi-Fi system for others.
4. Ensure that internet usage in labs and classrooms takes place only when necessary. If the internet facility needs to be used beyond school working hours, it must be done with the knowledge and permission of the school authorities. The person granting permission must ensure that, after use, the internet is properly switched off and the computer is shut down.
5. Guidelines regarding the proper use of the internet may be displayed in classrooms and laboratories.
6. Arrangements may be made in schools to specifically discuss the points mentioned in the preface and those related to cyber security included in the ICT textbooks.
7. When using CCTV systems in the school, the following matters should be taken into consideration -
   (a) The footage from CCTV cameras installed in schools must be securely stored in the DVR/NVR (Digital Video Recorder / Network Video Recorder) system available within the school itself. The footage should not be stored in cloud storage services belonging to private individuals or other unauthorized agencies under any circumstances.
   (b) The use of CCTV inside the classrooms including private servers should be avoided as it may violate students' privacy. However, this restriction does not apply during

special occasions such as examinations. In places where cameras are installed, a board clearly displaying "You are under CCTV surveillance" must be exhibited.

1. Social media activities related to the institution should be monitored by the Head of the Institution, and also ensure that these activities comply with students' privacy and data security requirements.
2. The privacy and security of the data collected in the school are very important. Therefore, information collected from students, others, or the government should not be shared with anyone without proper authorization.
3. The guidelines stated in the Government Order cited in Para 4 of this document (regarding digital content and the use of free software etc.,) must be complied with mandatorily.
4. Before using innovative technologies, systems, or other tools in schools as part of academic innovations, it must be ensured that they are consistent with the existing educational policies and perspectives, and prior approval must be obtained from the competent authorities.
5. While using students' Aadhaar information, the relevant government guidelines and provisions in various Acts regarding Aadhaar usage must be strictly followed. Such information should not be shared through spreadsheets or any other means under any circumstances.
6. Passwords for using various software and applications should be made accessible only to the persons responsible for them. Official passwords should not be autosaved.
7. To handle matters related to cyber security, a School Cyber Security Committee may be formed consisting of the Head of the Institution, staff representatives, a parent representative, and a student representative. A teacher may also be assigned the responsibility as the Cyber Safety Coordinator. School IT Coordinator, KITE Mentor may also be considered for this if required.
8. A system for reporting cyber security–related issues may be established in all schools. The Cyber Safety Coordinator may be assigned this responsibility. Information about the reporting officer may be displayed in the school.
9. The digital signature token, which is equivalent to the official seal, and its password must be kept securely and confidentially in the personal custody of the concerned official. Due to security risks, it should not be used in cyber cafés or public places. After use, one must log out of the portal and remove the token, and the login credentials of official portals such as SPARK and BiMS must be handled only by the respective officials.
10. A 'Cyber Safety Audit' may be conducted in schools at least once a year.

    (Guidelines for this shall be provided separately.)

7. Safeguards to be Ensured by the Teachers

1. Avoid using the internet directly in the classroom, instead necessary resources can be collected beforehand and used. However, resources available on portals prepared by the Education Department may be used directly in class.
2. Students should be allowed to use the internet only under the supervision of teachers or

other responsible staff.

3. Internet usage in the school should be limited to educational purposes, official requirements, and other study-related activities only.
4. When conducting internet-based activities in class groups, the activities should be planned in advance, and measures should be taken to ensure that students do not skip one activity to move to another.
5. Only resources whose authenticity has been verified—whether collected from the internet or prepared using AI tools—may be used for academic activities.
6. When using resources created with artificial intelligence (synthetically generated information), proper citation or reference must be provided. Similarly, any resource from other sources must also include references.
7. Passwords for various software and applications must be handled securely.
8. Students' data should not be handled in ways that violate privacy or data protection. Social media should not be used to collect sensitive information related to students.
9. Students should be given the opportunity to complete classroom/IT activities with the school itself. Equal access must be ensured for all the students so that there is no digital divide. Digital devices should not be made mandatory for completing homework assignments. However, online facilities such as Samagra Plus, Sahitham etc., may be provided for parents. If students do not have the necessary facilities at home to participate in programmes such as 'Key to Entrance', arrangements may be made at the school or elsewhere to enable their participation.

8. Safeguards Students Should Pay Attention To

1. The use of internet in schools should be strictly in accordance with the instructions of teachers.
2. If you receive offers that seem too good to be true, or suspicious links , such as messages claiming attractive offers or that you have won large prizes, do not click on them or respond to them.
3. Before downloading new games or social media apps, check the age rating and data permissions together and make sure they are suitable for you.
4. Be cautious, as free offers in games, limited-time deals, or temptations to quickly advance to higher levels may be "Dark patterns" designed to make you spend money unnecessarily.
5. Do not download, install, or use applications obtained from unreliable sources or websites.
6. Maintain self-control while playing online games. Be careful not to fall into challenges given by strangers or requests to share personal information or photos under any circumstances. In online games, avoid giving camera permissions and using live chat.
7. Never share live location or photos that can reveal your location on social media. Also, do not share sensitive information such as your mobile number.
8. Do not take or share photos or videos that display nudity. Such content can later lead to

blackmailing and cyber traps, so extreme caution should be exercised. Once an image is shared on the Internet, it is almost impossible to completely remove it later.

9. Do not share the passwords of your online accounts with anyone. Use different and strong passwords or passphrases for each account.
10. Do not threaten or mock anyone online. If someone mocks or threatens you, do not respond to them, instead block them immediately and inform your parents or teachers about it.
11. If you notice offensive messages, comments, or posts, take a screenshot and keep it. This is essential when filing a complaint.
12. Use technology honestly and safely. Avoid using AI tools to cheat in homework or projects that are part of the school curriculum, and do not download pirated movies or software without understanding the legal consequences.
13. View AI systems only as a tool for idea generation and do not depend on them entirely. Use the assistance obtained from them to develop your own thinking and problem-solving skills.
14. The information provided by AI should be verified by comparing it with other reliable sources (such as books, teachers, and trustworthy websites) before using it.
15. Do not store personal information or photos on computers used in public places such as schools or offices. Images may be morphed or misused in various ways. Similarly, do not use the information of other students or individuals in this manner.
16. Do not use pen drives or other storage devices on school or public computers without permission.
17. Do not hand over digital devices such as mobile phones, laptops or pen drives to strangers.
18. Never attempt to meet someone in person who you only know online without the presence of parent or guardian. Do not open emails or messages sent by people who are unfamiliar or untrustworthy.
19. Remember that forwarding false, harmful messages, images or videos is a criminal offence under cyber law.
20. Discuss openly with your parents or teachers about any problems, threats, or difficulties you encounter related to cyber use.
21. If you notice that someone has taken your photo without permission, inform your teachers or parents immediately.
22. When using AI tools, pay attention to fact-checking the information and identifying any bias.
23. Participate in cyber safety awareness activities in the community, such as programmes, quizzes, and seminars. Use these opportunities to read, understand, and share cyber security content included in ICT textbooks with others.
24. If there is no facility at home for activities like 'Key to Entrance' or submitting online applications, inform your teachers so that arrangements can be made to use the school lab.

25. Many cybercrimes targeting children occur in cyberspace. The major ones are listed separately in Annexure 1.

[In addition, more cybercrimes are explained on official websites (https://cybercrime.gov.in/) and in related documents issued by the government. Read and understand these resources.

9. Safeguards Parents Should Pay Attention To

1. Do not provide children with devices that are not approved by the school for use in school.
2. Ensure special supervision by parents when the child is using computers, mobile phones, or the Internet.
3. Make an effort to understand the use of new technologies. Keep your knowledge updated. Discuss openly with children about the use of social media and other digital platforms.
4. Observe whether there is excessive use of technology (internet, mobile phones) by children. If you notice any behavioural changes or signs that they may have fallen victim to cybercrimes, talk to them openly. Ask detailed questions without scaring them, report to the relevant authorities and provide counselling if necessary.
5. Be aware of modern scams, including those known as digital arrests..
6. Participate regularly in cyber safety awareness programs organised in schools, including Little KITEs units.
7. When providing children with laptops or mobile phones, ensure that the filters provided by web browsers or portals are activated. Explain the reason for this to the child to ensure a safe internet experience.
8. Pay extreme attention to whom children are connecting with online, as such contacts pose the highest risk of online grooming and exploitation.
9. Do not share PINs, passwords, or online banking credentials of parents' credit/debit cards with children.
10. Do not allow children to use parents' social media or email accounts.
11. Ensure that children adhere to the legal age limits for using social media platforms. Keep children's accounts always in 'Private' mode. To prevent strangers from viewing their photos or information.
12. Digital Footprint : Make children aware that once something is shared on the internet, it is difficult to remove completely. Advise them not to post anything that could affect future studies or employment.
13. As part of monitoring children's activities on computers or mobile devices, it is a good practice to check browsing history of apps after use. Tools such as ‘Family Center’ or ‘Family Link’ may be used.
14. Disable the 'In-app purchase' option on phones and allow children to use only secure 'Kid-Safe' apps.
15. Screen Time : The time spent using digital devices such as smartphones, computers, and television is called screen time. Excessive screen time can affect physical and mental

health. Use the 'Digital Well-being' or 'Screen Time' settings on your phone to set time limits for each app.

16. Maintain a friendly atmosphere with children. Encourage them to speak to you without fear if they face online difficulties (e.g., cyberbullying). Teach them safe digital habits.

10. General Guidelines

1. Enable two-factor authentication (2FA/MFA) on all social media and banking accounts. Two-factor authentication (2FA) provides an additional layer of security beyond the password for digital accounts. It is a process that requires two methods (factors) of verification to access an account. Examples include receiving a One-Time Password (OTP) on your mobile phone or using a security key when logging into a platform.
2. Avoid conducting banking transactions using public Wi-Fi networks at places like railway stations or cafés.
3. Set strong passwords for Wi-Fi routers at home.
4. When participating in video calls, ensure that the person you are speaking to is indeed your friend or relative. There is a possibility that the call could be a deepfake video generated using AI. If in doubt, verify the person's identity through another method, such as a regular phone call.
5. Social media netiquette: Do not post or comment anything that mocks, humiliates, or defames another person. Such actions are considered cyberbullying.
6. Regularly update the operating systems and applications on your phone and computer. This is essential to fix security vulnerabilities through security patches.
7. Download apps only from trusted sources such as the Play Store or App Store. Installing apps via APK files, links, or other third-party sources can lead to malware attacks and data theft. Avoid downloading apps from unauthorized websites. Check whether the permissions requested by an app are necessary before installation.
8. To detect and remove malware and viruses on mobile phones and computers, use the free antivirus/anti-malware tools provided by the Government of India's Botnet Cleaning and Malware Analysis Centre (Cyber Suraksha Kendra - CSK), available for download at the official website https://www.csk.gov.in/security-tools.html.
9. Uninstall apps that are not used for a long time. Such apps may pose a risk of data leakage.
10. Turn off location services on your phone when not needed. Avoid adding location tags when posting photos.
11. Always ensure that every link you click or action you take online is safe, remembering that "the internet never forgets and nothing truly disappears."

11. Password Security: General Guidelines

In order to ensure the security of digital accounts and devices, students, teachers, parents, and school authorities must all follow the password guidelines outlined below:

1. Strong password creation: Use passwords or passphrases that combine numbers, symbols, uppercase letters, and lowercase letters.
2. Avoid using the same password across accounts: Each account (banking, social media, official portals) should have a unique password; do not use the same password everywhere.
3. Confidentiality: Do not write passwords in diaries, phone notes, or anywhere accessible to others. Personal passwords must never be shared with friends or strangers under any circumstances.
4. Official security: Passwords for school software, applications, and other official systems should be accessible only to authorized personnel. Avoid using browser auto-save features for official passwords.
5. Two-factor authentication (2FA): Enable two-factor authentication (2FA/MFA), the second layer of account security, on all social media, banking, and official accounts.
6. Wi-Fi security: Ensure that school and home Wi-Fi networks have strong passwords and update them at regular intervals.
7. Habitual logout: Always log out properly from websites after using public computers or school labs.
8. Password protection: Secure photos and other confidential files with passwords before sharing them. This practice helps maintain data security when handling personal information at schools and at home.

12. Complaint Submission and Redressal Mechanism

Cyber security is a right for every individual. Students, teachers, and parents must have a basic understanding to recognize situations where this right is violated. They should also know how to respond when such incidents occur. In the event of a cyber attack or exploitation, the following legal measures should be taken without limiting the matter to the school level:

1. Inform the school cyber safety coordinator, head teacher, parent, or class teacher about the incident. (Stage 1)
2. Legal action: In cases of financial fraud or personal harm, immediately call 1930 or register a complaint via the National Cyber Crime Reporting Portal at [www.cybercrime.gov.in] (http://www.cybercrime.gov.in). (Stage 2)
3. Police complaint: For serious offenses such as morphing or blackmailing, file a complaint directly at the nearest police station or cyber cell. (Stage 3)
4. Helplines: Utilize the Kerala Police Cyber Helpline 1090 and Childline 1098 for assistance.

13. Data Protection Law and Children

Although the Digital Personal Data Protection Act (DPDP Act) 2023 has been passed by the central government, its rules have not yet been fully notified, and therefore the Act is currently implemented only partially. Nevertheless, the law emphasizes that utmost care must be taken while handling the data of children (below 18 years of age) and individuals facing physical or mental challenges.

Highlights of the Law

1. Data Fiduciary: Schools or apps that collect children's information fall under the definition of "Data Fiduciary" in the law. Accordingly, they are responsible for ensuring the security of the data collected, similar to internet platforms.
2. Penalty: Institutions violating the provisions of this law may be fined up to 200 crore INR.
3. IT Act 2000: Until the DPDP Act is fully implemented, relevant sections of the IT Act 2000 remain in force. Although Section 43A has been repealed, civil actions under Section 43 are still applicable.
4. Key provisions related to children's cyber safety and privacy under this law are provided in Annexure 2. Current rules and guidelines are issued specifically to enforce these provisions.
5. References to this law are also made in the IT Rules Amendment (2026). The important points are provided in Annexure 3. In addition, strict penalties for violations of children's cyber safety are also stipulated under the Indian Penal Code (IPC) and the Protection of Children from Sexual Offences (POCSO) Act.

14. Notification and Cyber Safety Auditing

The provisions outlined in the protocol must be effectively communicated to all students, teachers, and parents. To ensure this, training programs encompassing all stakeholder groups should be organised. Additionally, all related activities within the school must be subjected to regular auditing.

Cyber Safety Auditing

The misuse of internet facilities to exploit children at various levels is a matter of serious concern. Therefore, teachers, students, parents, and the wider community must act with vigilance to prevent such incidents.

Conducting cyber safety audits in schools enables the institution to operate with enhanced caution. For this purpose, a Cyber Safety Auditing Team can be constituted, including teachers, students, and parents. A sample checklist for auditing purposes is provided as Annexure 4.

Additionally, posters related to cyber safety can be displayed in school laboratories and common areas. Templates for these posters are provided in Annexures 5 and 6. When organising classes and seminars to raise awareness about digital safety, taking the Cyber Safety Pledge (Annexure 7) reinforces the associated message and strengthens the commitment to safe digital practices.

Annexures

Cyber Safety Protocol - 2026

for School Children in Cyber Kerala

Issued by:

Kerala Infrastructure and Technology for Education (KITE)

Poojappura, Thiruvananthapuram – 695012

www.kite.kerala.gov.in, contact@kite.kerala.gov.in, Ph: 0471-2529800

Annexure 1

Cybercrime, legal provisions, Prevention methods

Below is a list of some Cybercrimes explained in a way that is easy for children to understand. It also includes relevant sections of the IT Act 2000 and the New Indian Penal Code (BNS 2023).

Sl. No.	Crime	Description	Section	Precautions
1	Violation of Privacy	Copying or distributing images of someone's private parts without their consent.	IT Act Sec 66E.	Mask cameras when not in use.
2	Obscenity	This includes sharing and spreading inappropriate images or videos on the internet	IT Act Sec 67, 67A	Do not send inappropriate messages or pictures.
3	Cyber Stalking	Constantly monitoring someone online, harassing and threatening them with messages.	IT Act Sec 66, BNS Sec 78	Do not accept friend requests from strangers
4	Phishing	A method of stealing our confidential information by falsely claiming that it is from the bank or that we have won the lottery.	IT Act Sec 66D	Don't click on links offering prizes.
5	Deepfake	Using artificial intelligence to create fake videos or images by altering someone's face and voice.	IT Act Sec 66D, 66E	Do not share suspicious videos.
6	Identity Theft	This involves using someone else's password or other documents to commit fraud in their name.	IT Act Sec 66C	Use strong passwords.
7	Impersonation	Attempting to profit or cause harm by falsely impersonating someone else (for example, through a fake account).	IT Act Sec 66D	Check the authenticity of profiles.
8	Grooming	This is a way for adults to pretend to be friends and get close to children to trap them for bad things.	POCSO Act Sec 11(iv), 11(vi), 13, 15	Don't meet online friends alone in person.
9	Data Breach	This involves someone else obtaining our confidential information (photos, phone numbers, etc.) without our permission	DPDP Act 2023 IT Act Sec 66	Use only safe apps.
10	Camera Hacking	This is a way to steal your private information by secretly activating the camera on your phone or laptop without your knowledge.	IT Act Sec 66	Don't install unnecessary apps.

11	Sexting	Sending private pictures as messages is a crime. Even if it happens between children, it can be punished under the POCSO Act.	IT Act Sec 67, POCSO Act	Do not share private pictures online.
12	Cyber Bullying	This includes teasing and insulting someone through social media or gaming.		Be respectful to everyone online.
13	Fake News	Spreading false news is a crime. It can cause big problems in society.	IT Rules 2021/2026	Do not share information whose source is unknown
14	Hacking	This involves breaking into someone else's computer or internet account without their permission.	IT Act Sec 66	Do not share passwords with anyone.
15	Spoofing	This is a scam in which messages or emails are sent pretending to be someone else, hiding their real address.	IT Act Sec 66D	Do not click on suspicious links.
16	Sextortion	Taking private footage and demanding money or other things by threatening to release it is an extremely serious crime.	IT Act Sec 66, 67, BNS Sec 308	Do not give in to threats; immediately inform teachers or the police.
17	CSAM (Child Sexual Abuse Material)	Images, videos, audio recordings, etc. that sexually exploit or abuse children.	IT Act Sec 67B, 67B(b) POCSO Sec 15, 15(3)	Do not share private images online. If you see such material, please inform the relevant authorities.
18	Digital Arrest	Cyber fraud in which people pretend to be officers of investigative agencies like the police, Narcotics Bureau (NCB), and CBI, threatening to detain them through video calls, etc.	BNS Sec 61, 127, 204, 308, 319 (Since it is a new type of crime, there are no specific rules to deal with it.)	There is no such thing as 'digital arrest' in the Indian legal system. So don't be panic.
19	Trolling	It is a crime to make and distribute defamatory videos or messages in a way that mentally debilitates another person.	IT Act Sec 66	Don't create trolls that hurt others.
20	AI Grooming	While online grooming involves a person speaking directly to a child, in this case AI chatbots or deepfake technology are used for deception.	POCSO Act Sec 13-15	Avoid communicating online with strangers.

Annexure 2

The details of the offences related to children mentioned in the Digital Personal Data Protection Act (DPDP Act) are given in the table below.

Sl. No.	Offence	Description	Section	Precautions	Solution
1	Unauthorized data collection	It is a crime to collect children's personal information without parental consent.	Sec 9(1)	Provide parental consent via parents' email/phone number for apps used by children.	If information is collected incorrectly, you can request its correction or removal (Right to Erasure).
2	Tracking/ Monitoring	Technologies that monitor or track children's online behaviour should not be used.	Sec 9(3)	Turn on the 'Do Not Track' option in browsers. Opt out of location permissions.	File a complaint with the Data Protection Board (DPB).
3	Targeted Advertising	The law prohibits using children's information to display advertisements aimed at them.	Sec 9(3)	Turn off 'Ad Personalization' in the apps' privacy settings.	Use the reporting system on the platform.
4	Harmful data processing	It is punishable to use information in a way that affects the physical or mental health of children.	Sec 9(2)	Do not post children's pictures and school information on unfamiliar websites.	Complain through the National Cybercrime Portal (1930) or to the police.

Annexure 3

IT Rules Amendment 2026

Main Instructions

1. Identify AI content: Images, audio, and video created or altered using AI technology are called 'Synthetically Generated Information' (SGI). These may appear to be real, but they may be fake. It is imperative to check whether such content has the 'AI generated' label.

2. Beware of fake footage: It is illegal to fake someone's appearance or voice using AI. Do not forward such unauthentic videos or voice clips to anyone.

3. Urgent reporting and action: Report child abuse, unauthorized private footage, and deepfakes immediately. The new law requires social media platforms to take action on such complaints within two hours.

Annexure 4

Cyber Safety Audit- Checklist

1	Separate logins have been created for classes and/or teachers on the school's computers.	
2	All computers and laptops are password protected.	
3	The school's Wi-Fi is secured with a strong password. Additionally, this password is changed at regular intervals to ensure security.	
4	The school email is operated on a government-sanctioned system. The email is protected with a strong password.	
5	The school email is used only by the head teacher/designated person.	
6	It has been ensured that the various e-governance systems used by the school are used only by authorized persons.	
7	It has been ensured that children's personal information is collected only on websites designated by the government.	
8	It has been ensured that there is no privacy violation when sharing content involving children on social media.	
9	The digital information collected by the school is backed up at regular intervals.	
10	The screens of computers/laptops used by children are set up in a way that everyone can see them.	
11	Training on cybersecurity has been provided to teachers, students, and parents at intervals prescribed by the government.	
12	A board containing instructions on what to do if you are a victim of any type of cybercrime, has been displayed in public spaces.	

[More items may be added depending on the school's situation.]

Annexure 5

Notice to Be Displayed in Computer Labs Regarding Safe Internet Usage

Safe Internet Usage

✔ Things to Follow

- Use only the educational websites recommended by your teacher.
- Use strong passwords for all accounts.
- Log out of websites after use.
- Open only secure websites with "https://".
- Inform your teacher immediately if you find any suspicious content.
- Behave respectfully towards everyone online.
- Follow copyright laws when downloading content.
- Remember your digital footprint: everything you post online can become a permanent digital record. Think twice before posting.

✘ Things Not to Do

- Do not share personal information such as address, phone number, passwords, or home location.
- Do not download software or apps without permission.
- Do not send offensive or insulting messages.
- Do not use social media during school hours.

Cybercrime Reporting Number: 1930

Annexure 6

Notice to be Displayed on School Notice Board Regarding Cyber Safety

Cyber Safe School

- Students of this school shall use the internet only under the supervision of teachers.
- Students shall be regularly guided on safe and responsible use of the Internet.
- Student data shall be shared only with government-approved websites.
- Only content that is free to use in accordance with copyright law shall be downloaded from the Internet.
- Regular cyber safety training shall be provided to teachers, students, and parents.
- Any observed cybercrime incidents shall be reported to the relevant authorities for legal action.
- Only free and open-source software shall be used on the school computers.

Cybercrime Reporting Number: 1930

Annexure 7
Cyber Safe Pledge

I pledge to grow as a responsible citizen in the digital world.

I will keep my personal information and passwords secure and confidential. I will also protect personal information related to my family. I will encourage my family members to adopt such security practices as well. I affirm that I will not establish personal relationships with strangers I meet on the internet, and I will not click on unsecured or suspicious links.

I will not insult or ridicule my classmates or others on online platforms. If I come across any traps or difficulties in the cyber world, I will report them immediately to my teachers or parents without hiding or concealing them.

I hereby pledge that while using digital devices for learning and entertainment, I will adhere to a proper time schedule and utilize technology solely for the well-being of myself and society.

Cyber Safety Protocol - 2026
for School Children in Cyber Kerala

Issued by:

Kerala Infrastructure and Technology for Education (KITE)

Poojappura, Thiruvananthapuram – 695012

www.kite.kerala.gov.in, contact@kite.kerala.gov.in, Ph: 0471-2529800

CYBER SAFETY PROTOCOL 2026

for School Children

GENERAL EDUCATION DEPARTMENT
GOVERNMENT OF KERALA

KERALA INFRASTRUCTURE AND TECHNOLOGY FOR EDUCATION

Kerala Infrastructure & Technology for Education (KITE)
Poojappura, Thiruvananthapuram - 695012
www.kite.kerala.gov.in, contact@kite.kerala.gov.in
Phone : 0471 2529800