"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

സ്കൂൾ കുട്ടികൾക്കുവേണ്ടിയുള്ള

സൈബർ സേഫ്റ്റി പ്രോട്ടോക്കോൾ

AI Generated Image

പൊതുവിദ്യാഭ്യാസവകുപ്പ്
കേരള സർക്കാർ

KERALA INFRASTRUCTURE AND TECHNOLOGY FOR EDUCATION

കേരള ഇൻഫ്രാസ്ട്രക്ചർ & ടെക്നോളജി
ഫോർ എഡ്യൂക്കേഷൻ (കൈറ്റ്)
പൂജപ്പുര, തിരുവനന്തപുരം - 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

നം.കൈറ്റ്/2026/1605 (1) തീയതി : 07.03.2026

സ്കൂൾ കുട്ടികൾക്കുവേണ്ടിയുള്ള സൈബർ സേഫ്റ്റി പ്രോട്ടോകോൾ

വിഷയം:- കൈറ്റ് - കേരളത്തിലെ പൊതുവിദ്യാലയങ്ങൾക്കുള്ള ഭേദഗതി ചെയ്ത സൈബർ സുരക്ഷാ പ്രോട്ടോകോൾ 2026 പുറപ്പെടുവിക്കുന്നു.

സൂചന:-
1. സ്കൂൾ കുട്ടികൾക്ക് വേണ്ടിയുള്ള 23.02.2019 ലെ KITE/2019/1605(2) നമ്പർ സൈബർ സേഫ്റ്റി പ്രോട്ടോകോൾ
2. 30.01.2023-ലെ സഉ(സാധാ) നം.818/2023/GEDN
3. കൈറ്റ് ഡയറക്ടർ ബോർഡിന്റെ 13.04.2023-ലെ 22-ാം യോഗത്തിന്റെയും 02.02.2026 ലെ 32-ാം യോഗത്തിന്റെയും മിനിറ്റ്സ്.
4. പൊതുവിദ്യാഭ്യാസ വകുപ്പിലെ ഐടി സാങ്കേതിക സമിതിയുടെ 06.03.2026 ലെ യോഗത്തിന്റെ മിനിറ്റ്സ്

പതിമൂന്നാം കേരള നിയമസഭയുടെ സ്ത്രീകളുടേയും കുട്ടികളുടേയും വികലാംഗരുടേയും ക്ഷേമം സംബന്ധിച്ച സമിതിയുടെ ശുപാർശ അനുസരിച്ച് സ്കൂൾ കുട്ടികൾക്കായി സൈബർ സേഫ്റ്റി പ്രോട്ടോകോൾ സൂചന 1 പ്രകാരം കൈറ്റ് പുറപ്പെടുവിച്ചിട്ടുണ്ട്. സ്കൂളുകൾക്കും ഓഫീസുകൾക്കും ഉള്ള പുതുക്കിയ ഐസിടി മാർഗനിർദ്ദേശങ്ങൾ പുറത്തിറക്കിയ സൂചന 2-ലെ സർക്കാർ ഉത്തരവിൽ, സ്കൂളുകൾക്കായി പുറപ്പെടുവിച്ചിരിക്കുന്ന സൈബർ സേഫ്റ്റി പ്രോട്ടോകോൾ കൃത്യമായി പാലിക്കേണ്ടതാണ് എന്ന് നിഷ്കർഷിച്ചിട്ടുണ്ട്. സൂചന 3 പ്രകാരമുള്ള യോഗങ്ങളിൽ സൈബർ സേഫ്റ്റി പ്രോട്ടോകോൾ പുതുക്കി പ്രസിദ്ധീകരിക്കാൻ കൈറ്റിനെ ചുമതലപ്പെടുത്തിയിട്ടുണ്ട്.

പാഠ്യപദ്ധതി പരിഷ്കരണത്തിന്റെ ഭാഗമായി 2024 മുതൽ പരിഷ്കരിച്ച ഐസിടി പാഠപുസ്തകങ്ങളിലും ലിറ്റിൽ കൈറ്റ്സ് പരിശീലനങ്ങളിലും സൈബർ സുരക്ഷ മുന്തിയ പ്രാധാന്യത്തോടെ ഉൾപ്പെടുത്തിയിട്ടുണ്ട്. പുതിയ പ്രോട്ടോക്കോളിന് സ്വീകരിക്കേണ്ട സമീപനം ഈ രംഗത്തെ അന്തർദേശീയ മാതൃകകളും പഠനങ്ങളും രാജ്യത്തെ നിയമങ്ങളും വിശദമായി അപഗ്രഥനം ചെയ്ത് സൈബർ സുരക്ഷാ പ്രോട്ടോകോളിന്റെ കരട് കൈറ്റ് തയ്യാറാക്കുകയും ആയതിന് സൂചന 4 ലെ സർക്കാർ നിയമിച്ച ഐടി സാങ്കേതിക സമിതി അനുമതി നൽകുകയും ചെയ്തു.

ഈ പശ്ചാത്തലത്തിൽ സൂചന 1 ലെ കേരളത്തിലെ സ്കൂളുകൾക്കുള്ള സൈബർ സേഫ്റ്റി പ്രോട്ടോകോൾ ഭേദഗതി ചെയ്ത് പുതുക്കിയ സൈബർ സേഫ്റ്റി പ്രോട്ടോകോൾ-2026 ഇതോടൊപ്പം പ്രസിദ്ധീകരിക്കുന്നു. പ്രോട്ടോകോൾ കാലാനുസൃതമായി പുതുക്കാനും മാർഗനിർദ്ദേശങ്ങൾ നടപ്പാക്കാനും കൈറ്റ് സംവിധാനം ഏർപ്പെടുത്തുന്നതാണ്.

കെ. അൻവർ സാദത്ത്
ചീഫ് എക്സിക്യൂട്ടീവ് ഓഫീസർ

ഉള്ളടക്കം

പേജ്

03 .....ആമുഖം

04 .....സൈബർ സേഫ്റ്റി പ്രോട്ടോക്കോൾ - ഉദ്ദേശ്യങ്ങൾ

06 .....സൈബർ സുരക്ഷ ഐ.സി.ടി. പാഠപുസ്തകത്തിൽ

07 .....പ്രോട്ടോക്കോളിന്റെ പരിധിയും ഗുണഭോക്താക്കളും

08 .....സ്ഥാപനമേധാവി ഉറപ്പുവരുത്തേണ്ട കാര്യങ്ങൾ

10 .....അധ്യാപകർ ഉറപ്പുവരുത്തേണ്ടത്

11.....വിദ്യാർഥികൾ ശ്രദ്ധിക്കേണ്ട കാര്യങ്ങൾ

13 .....രക്ഷിതാക്കൾ ശ്രദ്ധിക്കേണ്ട കാര്യങ്ങൾ

14 .....പൊതുനിർദേശങ്ങൾ

15 .....പാസ്‌വേഡ് സുരക്ഷ : പൊതുവായ മാർഗനിർദേശങ്ങൾ

16 .....പരാതി സമർപ്പിക്കലും പരിഹാര രീതിയും

16 .....ഡാറ്റാ സംരക്ഷണനിയമവും കുട്ടികളും

17 .....അറിയിക്കലും സൈബർ സേഫ്റ്റി ഓഡിറ്റിങ്ങും

18. .....അനുബന്ധം 1 : സൈബർ കുറ്റകൃത്യങ്ങൾ, നിയമവകുപ്പുകൾ, പ്രതിരോധ മാർഗങ്ങൾ

20 .....അനുബന്ധം 2 : DPDP Act ൽ പരാമർശിച്ച കുട്ടികളുമായി ബന്ധപ്പെട്ട കുറ്റകൃത്യങ്ങളും പ്രതിരോധവും

21 .....അനുബന്ധം 3 : ഐ.ടി. ചട്ടഭേദഗതി (2026) - പ്രധാന നിർദേശങ്ങൾ

22 .....അനുബന്ധം 4 : സൈബർ സെക്യൂരിറ്റി ഓഡിറ്റ് - ചെക്ക്‌ലിസ്റ്റ്

23 .....അനുബന്ധം 5 : കമ്പ്യൂട്ടർ ലാബിൽ പ്രദർശിപ്പിക്കേണ്ട നോട്ടീസ്

24 .....അനുബന്ധം 6 : നോട്ടീസ് ബോർഡിൽ പതിക്കേണ്ട പോസ്റ്റർ - മാതൃക

25 .....അനുബന്ധം 7 : സൈബർ സുരക്ഷാ പ്രതിജ്ഞ

സൈബർ സേഫ്റ്റി പ്രോട്ടോക്കോൾ

1. ആമുഖം

ഡിജിറ്റൽ ലോകം നമ്മുടെ ജീവിതത്തിന്റെ അവിഭാജ്യഘടകമായി മാറിയിരിക്കുന്ന ഈ കാലഘട്ടത്തിൽ, ഇന്റർനെറ്റും ഡിജിറ്റൽ സംവിധാനങ്ങളും ഉപയോഗിക്കുമ്പോൾ പാലിക്കേണ്ട സുരക്ഷാ മാനദണ്ഡങ്ങളെക്കുറിച്ചുള്ള അറിവ് വളരെ പ്രധാനമാണ്. പഠനപ്രവർത്തനങ്ങളുടെ ഭാഗമായി മാത്രമല്ല, വിനോദത്തിനായും വിവരവിനിമയത്തിനായുമെല്ലാം കുട്ടികൾ ആധുനിക സാങ്കേതികവിദ്യാ ഉപകരണങ്ങൾ ഉപയോഗിക്കുന്നുണ്ട്. പുതിയ അവസരങ്ങൾക്കും പഠനരീതികൾക്കും വഴിയൊരുക്കുന്ന ഈ സാങ്കേതിക പുരോഗതി, അതിനൊപ്പം ഗൗരവമുള്ള വെല്ലുവിളികളും സൃഷ്ടിക്കുന്നു. നിർമ്മിത ബുദ്ധി (Artificial Intelligence) ഉൾപ്പെടെയുള്ള ആധുനിക സാങ്കേതികവിദ്യകൾ വിദ്യാഭ്യാസരംഗത്ത് വലിയ രീതിയിൽ ഉപയോഗപ്പെടുത്തുന്ന സാഹചര്യത്തിൽ, അവയുടെ ഗുണങ്ങളോടൊപ്പം ഉത്തരവാദിത്തപരവും സുരക്ഷിതവുമായ ഉപയോഗവും ഉറപ്പാക്കേണ്ടത് അനിവാര്യമാണ്. ഇതിനായി ഡിജിറ്റൽ ഉള്ളടക്കം (Content), ഡിജിറ്റൽ ഉള്ളടക്കവുമായുള്ള സമ്പർക്കം (Contact), സൈബർ ലോകത്തെ പെരുമാറ്റം (Conduct), കരാർ (Contract) എന്നിങ്ങനെയുള്ള വിവിധ മേഖലകളിലായി വ്യാപിച്ചുകിടക്കുന്ന അപകടസാധ്യതകളെ സമഗ്രമായി അഭിസംബോധന ചെയ്യേണ്ടതുണ്ട്.

കുട്ടികളും രക്ഷിതാക്കളും അധ്യാപകരും അനധ്യാപകരും ഉൾപ്പെടുന്ന സ്കൂൾസമൂഹം ഡിജിറ്റൽ സാങ്കേതികവിദ്യകൾ ഉപയോഗിക്കുമ്പോൾ വിവിധതരത്തിലുള്ള ചൂഷണങ്ങളെ നേരിടേണ്ടി വന്നേക്കാം. എ.ഐ. വശീകരണം (AI Grooming), ഡീപ്ഫേക്ക് വഴി ഭീഷണിപ്പെടുത്തൽ (Deepfake blackmailing), ശബ്ദാനുകരണം (Voice Cloning), ഓൺലൈൻ പ്രലോഭനം (Online luring), സൈബർ ഭീഷണി (Cyber bullying), ദോഷകരമായ ഉള്ളടക്കങ്ങൾ നിർമ്മിക്കൽ (Harmful Content) തുടങ്ങിയവ ഇതിൽ ഉൾപ്പെടുന്നു. മാത്രമല്ല, ഡിജിറ്റൽ ഉപകരണങ്ങളുടെ അമിത ഉപയോഗം കുട്ടികളുടെ ആരോഗ്യം, ഭാവനാശേഷി, സാമൂഹിക പെരുമാറ്റം, പഠനരീതി, മാനസികാരോഗ്യം എന്നിവയെ കൂടി പ്രതികൂലമായി ബാധിക്കുമെന്നും ആശങ്കകളുണ്ട്.

നൂതന സാങ്കേതികവിദ്യകൾ വ്യാപകമാകുമ്പോൾ ഉണ്ടായേക്കാവുന്ന ഇത്തരം വെല്ലുവിളികളെ നേരിടുന്നതിനുപകരം അനാവശ്യ ഭീതി പടർത്തി ഇവയുടെ ഉപയോഗത്തിൽ നിന്നും മാറ്റിനിർത്തുന്ന സാഹചര്യവും ഒഴിവാക്കേണ്ടതുണ്ട്. വിദ്യാഭ്യാസരംഗത്ത് സൈബർസുരക്ഷ ഉറപ്പാക്കാനുള്ള ക്രിയാത്മകമായ ഇടപെടൽ കേരള ഇൻഫ്രാസ്ട്രക്ചർ & ടെക്നോളജി ഫോർ എഡ്യൂക്കേഷൻ (കൈറ്റ്) ബഹുമുഖതലത്തിൽ നടത്തിവരുന്നുണ്ട്. ഒന്നു മുതൽ പത്തു വരെ ക്ലാസുകളിലേക്കുള്ള ഐ.സി.ടി. പാഠപുസ്തകങ്ങൾ, ഡിജിറ്റൽ ഉള്ളടക്കം ലഭ്യമാക്കാനും അക്കാദമിക മോണിറ്ററിംഗിനുമുള്ള സമഗ്ര പ്ലസ് പോർട്ടൽ, ഇന്ത്യയിലെ കുട്ടികളുടെ ഏറ്റവും വലിയ ഐ.ടി. കൂട്ടായ്മയായ ലിറ്റിൽ കൈറ്റ്സ് ക്ലബ്ബ്, ഇന്ത്യയിലെ ആദ്യത്തെ സമഗ്ര വിദ്യാഭ്യാസ ചാനലായ കൈറ്റ് വിക്ടേഴ്സ് തുടങ്ങിയവയിലൂടെ സൈബർ ചതിക്കുഴികൾ തിരിച്ചറിയാനും സൈബർ കുറ്റകൃത്യങ്ങളെ പ്രതിരോധിക്കാനും പരിഹാരം കാണാനും വിപുലമായ പദ്ധതികൾ നേരത്തെ തന്നെ നടപ്പിലാക്കിയിട്ടുണ്ട്.

സ്കൂളുകളിൽ 'സൈബർ സേഫ്റ്റി ക്ലിനിക്കുകൾ' സ്ഥാപിക്കുന്നത് ഇതിന്റെ ഭാഗമായി നടക്കുന്ന പ്രധാനപ്പെട്ട പ്രവർത്തനമാണ്. കുട്ടികൾക്കും അധ്യാപകർക്കും രക്ഷിതാക്കൾക്കും സൈബർ സുരക്ഷയിൽ കൈറ്റ് പ്രായോഗികപരിശീലനം നൽകി വരുന്നുണ്ട്. കൃത്യമായ പരിശീലന മൊഡ്യൂളുകളും റിസോഴ്സുകളും കേന്ദ്രീകൃതമായി നിർമ്മിച്ചുനൽകിയും കൃത്യമായ മോണിറ്ററിങ്ങോടും കൂടിയാണ് ഇത്തരം പരിശീലനങ്ങൾ നടത്തുന്നത്. ഇതിനായി

ദേശീയ-അന്തർ ദേശീയ തലങ്ങളിൽ വൈദഗ്ധ്യവും വിശ്വാസ്യതയുമുള്ള സ്ഥാപനങ്ങളുടെയും വ്യക്തികളുടെയുമെല്ലാം സേവനം കൈറ്റ് പ്രയോജനപ്പെടുത്തിവരുന്നു.

സ്മാർട്ട്ഫോൺ ഉൾപ്പടെയുള്ള വ്യത്യസ്ത ഗാഡ്ജെറ്റുകളിൽ നിർമ്മിതബുദ്ധി (എ.ഐ.) സങ്കേതങ്ങൾ വ്യാപകമായിക്കൊണ്ടിരിക്കുന്ന സാഹചര്യത്തിൽ ഡിജിറ്റൽ ഡിവൈഡ് വ്യക്തികളുടെ അവകാശങ്ങളെ ചൂഷണം ചെയ്തതുപോലെ എ.ഐ. ഡിവൈഡിലൂടെയും വ്യക്തികൾ ചൂഷണത്തിനിരയായേക്കാം. ഇത് തിരിച്ചറിഞ്ഞുകൊണ്ട് കേരളത്തിലെ വിദ്യാർഥികളും രക്ഷിതാക്കളും ഈ പരിമിതിയിൽ അകപ്പെടാത്ത വിധത്തിലുള്ള കൈത്താങ്ങ് നൽകുന്നതിനുള്ള പ്രവർത്തനങ്ങളും കൈറ്റ് ആവിഷ്കരിച്ച് നടപ്പിലാക്കുന്നുണ്ട്. ഇതിന്റെ ഭാഗമായി അധ്യാപകർക്കും കുട്ടികൾക്കും കൈറ്റ് നേരിട്ട് പരിശീലനം നൽകുന്നതോടൊപ്പം ലിറ്റിൽ കൈറ്റ്സ് കുട്ടികളെ പരിശീലകരാക്കി രക്ഷിതാക്കൾക്കും എ.ഐ. പരിശീലനം നൽകിവരുന്നു.

സാങ്കേതികവിദ്യയിലുണ്ടാകുന്ന ദ്രുതഗതിയിലുള്ള മാറ്റങ്ങൾ വിദ്യാഭ്യാസപ്രക്രിയയുടെ ഭാഗമാക്കുന്നതിനായി ലിറ്റിൽ കൈറ്റ്സ് അംഗങ്ങൾ, കൈറ്റ് മെന്റർമാർ, സ്കൂൾ ഐ.ടി. കോർഡിനേറ്റർമാർ, വിദ്യാഭ്യാസ ഓഫീസർമാർ എന്നിവർക്ക് കൃത്യമായ ഇടവേളകളിൽ വിദഗ്ധ പരിശീലനം 'കൈറ്റ്' നൽകി വരുന്നു. സൈബർ ലോകത്തെ അടിയന്തര സാഹചര്യങ്ങളിൽ സ്വീകരിക്കേണ്ട മുൻകരുതലുകളും, വെല്ലുവിളികളെ നേരിടുന്നതിനുള്ള പ്രായോഗികമായ പ്രതിരോധ മാർഗങ്ങളും പരിശീലന പരിപാടികളുടെ പ്രധാന ഭാഗമാണ്.

സംസ്ഥാനത്തെ വിദ്യാലയങ്ങളിൽ ഐ.സി.ടി. പഠനം ആരംഭിച്ച കാലംമുതൽ കമ്പ്യൂട്ടറുകളും അനുബന്ധ ഉപകരണങ്ങളും ഇന്റർനെറ്റും ഫലപ്രദമായും സുരക്ഷിതമായും ഉപയോഗിക്കുന്നതിനുള്ള നിർദേശങ്ങളും പരിശീലനങ്ങളും വിവിധ തലങ്ങളിൽ നൽകിവരുന്നുണ്ട്. അവയിൽ പ്രധാനപ്പെട്ടവ ചുവടെ ചേർക്കുന്നു.

1. വിദ്യാഭ്യാസവകുപ്പ് തയ്യാറാക്കിയ വിവരവിനിമയ സാങ്കേതികവിദ്യ(ഐ.സി.ടി.) പാഠപുസ്തകങ്ങളിലെ സൈബർസുരക്ഷയുമായി ബന്ധപ്പെട്ട പാഠഭാഗങ്ങൾ.

2. സ്കൂളുകൾക്കും വിദ്യാഭ്യാസ ഓഫീസുകൾക്കും വേണ്ടി പൊതുവിദ്യാഭ്യാസവകുപ്പ് പുറപ്പെടുവിച്ച മാർഗനിർദേശങ്ങൾ അടങ്ങുന്ന 30.01.2023-ലെ സ.ഉ(സാധാ) നം.818/2023/GEDN നമ്പർ സർക്കാർ ഉത്തരവ്.

3. പൊതുവിദ്യാഭ്യാസ സംരക്ഷണ യജ്ഞത്തിന്റെ ഭാഗമായുള്ള ഹൈടെക് സ്കൂൾ പദ്ധതിയിലുൾപ്പെടുത്തി ക്ലാസ് മുറികൾ ഹൈടെക് ആക്കുന്നതിന് നൽകുന്ന ഉപകരണങ്ങളും സൗകര്യങ്ങളും സേവനങ്ങളുമെല്ലാം പ്രയോജനപ്പെടുത്തുന്നതിന് 10.01.2018 തീയതിയിലെ സ.ഉ.(സാധാ) നം. 165/2018/പൊ.വി.വ. നമ്പർ സർക്കാർ ഉത്തരവും ഇതിനനുസൃതമായി കൈറ്റും സ്കൂളുകളും തമ്മിൽ ഒപ്പു വച്ചിട്ടുള്ള ധാരണാപത്രവും.

4. ലിറ്റിൽ കൈറ്റ്സ് ക്ലബുകൾ വഴി 4 ലക്ഷം രക്ഷിതാക്കൾക്ക് സൈബർ സുരക്ഷാ പരിശീലനം നൽകുന്നതിനുള്ള 'അമ്മ അറിയാൻ' എന്ന പേരിൽ തയ്യാറാക്കിയ മൊഡ്യൂൾ.

2. സൈബർ സേഫ്റ്റി പ്രോട്ടോക്കോൾ - ഉദ്ദേശ്യങ്ങൾ

1. അധ്യാപകരുടെയും രക്ഷിതാക്കളുടെയും ഉത്തരവാദിത്തത്തിൽ സുരക്ഷിതമായ ഡിജിറ്റൽ പഠനാന്തരീക്ഷം (Safe Digital Learning Environment) കുട്ടികൾക്ക് ലഭ്യമാക്കുക.

2. സൈബർസുരക്ഷ സ്കൂളുകളിലെ ഒരുവിഭാഗത്തിന്റെ മാത്രമല്ല മുഴുവൻ സംവിധാനത്തിന്റെയും ഉത്തരവാദിത്തമാണ്.

3. കുട്ടികൾക്കും മറ്റു വ്യക്തികൾക്കും എതിരെ നടക്കുന്ന സൈബർ അതിക്രമങ്ങളെ (Stalking, Harassment, etc.) ഫലപ്രദമായി പ്രതിരോധിക്കുന്നതിനും നിയമസഹായങ്ങൾ തേടുന്നതിനും കുട്ടികളെയും അധ്യാപകരെയും സ്ഥാപന മേധാവികളെയും രക്ഷിതാക്കളെയും പ്രാപ്തരാക്കുക.

4. പ്രായത്തിനും വികാസത്തിനും അനുയോജ്യമല്ലാത്ത ഓൺലൈൻ ഉള്ളടക്കങ്ങൾ (Content Risk) തിരിച്ചറിയാനും ഒഴിവാക്കാനും കുട്ടികളെ പ്രാപ്തരാക്കുക.

5. എ.ഐ ഗ്രൂമിംഗ്, ഡീപ്ഫേക് ബ്ലാക്മെയിലിംഗ്, വിഷിംഗ് (വോയ്സ് ക്ലാണിംഗ്), ഹാക്കിംഗ്, ഐഡന്റിറ്റി തെഫ്റ്റ് തുടങ്ങിയ ഓൺലൈൻ ചൂഷണങ്ങളെ (Contact Risk) കുറിച്ച് കുട്ടികളെയും രക്ഷിതാക്കളെയും ബോധവാന്മാരാക്കുകയും ഇതിലൂടെ കുട്ടികൾക്കെതിരെയുള്ള ഓൺലൈൻ അതിക്രമങ്ങൾ തടയുകയും ചെയ്യുക.

6. ഡിജിറ്റൽ സ്വാതന്ത്ര്യത്തോടൊപ്പം എന്ത് കാണണം, എന്ത് പങ്കിടണം, എന്ത് ഒഴിവാക്കണം, ഓൺലൈൻ ലോകത്ത് എങ്ങനെ സുരക്ഷിതമായി ഇടപഴകണം (Conduct Risk) തുടങ്ങിയ ഡിജിറ്റൽ മര്യാദകൾ (Netiquette) ശീലിപ്പിച്ച് കുട്ടികളിൽ മികച്ച സൈബർ സംസ്കാരം (Cyber Culture) വളർത്തിയെടുക്കുക.

7. ഓൺലൈൻ ഇടങ്ങളിൽ വ്യക്തികളുടെ സ്വകാര്യ വിവരങ്ങൾ (പേര്, വിലാസം, ഫോട്ടോ, ഫോൺ നമ്പർ, അക്കൗണ്ട് വിവരങ്ങൾ തുടങ്ങിയവ) മറ്റുള്ളവർ ദുരുപയോഗം ചെയ്യാതെ സംരക്ഷിക്കുന്നതിനെക്കുറിച്ച് അവബോധമുണ്ടാക്കുക.

8. ഡിജിറ്റൽ വിവരങ്ങളെ വിമർശനാത്മക ചിന്തയോടെ (Critical Thinking) സമീപിക്കുന്നതിനും അവയുടെ നിജസ്ഥിതി പരിശോധിക്കുന്നതിനും അതുവഴി വ്യാജവാർത്തകളും വിവരങ്ങളും തിരിച്ചറിയുന്നതിനും കുട്ടികളെ പ്രാപ്തരാക്കുക.

9. ജനറേറ്റീവ് എ.ഐ. ടൂളുകൾ ഉപയോഗിക്കുമ്പോൾ വ്യക്തിഗതമോ ഔദ്യോഗികമോ ആയ രഹസ്യവിവരങ്ങൾ പങ്കുവെക്കുന്നതിലെ അപകടങ്ങളെക്കുറിച്ച് അവബോധമുണ്ടാക്കുക.

10. ഡിജിറ്റൽ ഇടങ്ങളിലെ കുറ്റകൃത്യങ്ങൾ തടയുന്നതിനും നിയന്ത്രിക്കുന്നതിനുമുള്ള ഐ.ടി. ആക്ട് (IT Act 2000), ഡിജിറ്റൽ വ്യക്തിഗത വിവരസംരക്ഷണ നിയമം (DPDP Act 2023), ഐ.ടി. ചട്ട ഭേദഗതി (2006) തുടങ്ങിയവയെക്കുറിച്ച് എല്ലാവരെയും ബോധവാന്മാരാക്കുകയും അതോടൊപ്പം, സൈബർ ആക്രമണങ്ങൾക്കും എ.ഐ. ദുരുപയോഗങ്ങൾക്കും എതിരെ നിയമപരമായ പരിരക്ഷ തേടാനുമുള്ള ശേഷി വ്യക്തികളിൽ വളർത്തിയെടുക്കുകയും ചെയ്യുക.

11. സ്വതന്ത്ര സോഫ്റ്റ്വെയറുകളുടെ (Free and Open-Source Software - FOSS) പ്രയോജനങ്ങളെക്കുറിച്ചും ഇതിന്റെ വിപുലമായ സാധ്യതകളെ കുറിച്ചും അധ്യാപകർക്കും വിദ്യാർഥികൾക്കും പൊതു സമൂഹത്തിനും അവബോധമുണ്ടാക്കുക.

12. സുരക്ഷിതവും, ചെലവുകുറഞ്ഞതും, വിദ്യാഭ്യാസ ആവശ്യങ്ങൾക്കനുയോജ്യമായി പരിഷ്കരിക്കാവുന്നതുമായ സ്വതന്ത്ര സോഫ്റ്റ്വെയറുകളുടെ ഉപയോഗം അക്കാദമിക രംഗത്ത് പ്രോത്സാഹിപ്പിക്കുകയും, അതിലൂടെ ഡിജിറ്റൽ സ്വയം പര്യാപ്തത (Digital Autonomy) കൈവരിക്കുകയും ചെയ്യുക.

13. ഡിജിറ്റൽ നിയമങ്ങൾ പാലിക്കാനും സൈബർ പ്രതിസന്ധി ഘട്ടങ്ങളിൽ നേതൃത്വം നൽകാനും കഴിയുന്ന ഉത്തരവാദിത്തമുള്ള ഡിജിറ്റൽ സംസ്കാരമുള്ളവരായി (Digital culture) കുട്ടികളെ വളർത്തിയെടുക്കുക.

3. സൈബർ സുരക്ഷ ഐ.സി.ടി. പാഠപുസ്തകത്തിൽ

പ്രൈമറി തലത്തിലെയും സെക്കണ്ടറി തലത്തിലെയും പാഠപുസ്തകങ്ങളിൽ സൈബർ സുരക്ഷയുമായി ബന്ധപ്പെട്ട ഉള്ളടക്കം ചേർത്തിട്ടുണ്ട്. പാഠ്യപദ്ധതി ചട്ടക്കൂടിൽ പരാമർശിച്ചതു പ്രകാരമാണ് ഇതുൾപ്പെടുത്തിയിട്ടുള്ളത്. പാഠപുസ്തകങ്ങളിൽ ഉൾപ്പെടുത്തിയ ഏതാനും വസ്തുതകൾ താഴെ നൽകിയിരിക്കുന്നു.

1. അഞ്ചാം ക്ലാസിലെ 'ഇൻറർനെറ്റിൽ തിരയുമ്പോൾ' എന്ന അധ്യായത്തിൽ വ്യാജവാർത്തകൾ എങ്ങനെ കൈകാര്യം ചെയ്യണമെന്നും സ്ക്രീൻസമയം ഫലപ്രദമായി ക്രമീകരിക്കേണ്ടതിന്റെ ആവശ്യകതയും പരിചയപ്പെടുത്തുന്നു.

2. ഏഴാം ക്ലാസിലെ '**തിരയാം കണ്ടെത്താം**' എന്ന പാഠഭാഗത്ത് പകർപ്പവകാശം, നിത്യജീവിതത്തിൽ ഇന്റർനെറ്റിന്റെ സ്വാധീനം, നിർമ്മിത ബുദ്ധി നമ്മുടെ ഇന്റർനെറ്റ് ഉപയോഗത്തെ എങ്ങനെ സ്വാധീനിക്കുന്നു, സൈബർലോകത്തെ ശരിയായ ഇടപെടൽ എന്നതിനെക്കുറിച്ചെല്ലാം വിവരിക്കുന്നു.

3. എട്ടാം ക്ലാസിലെ '**അതിരുകളില്ലാത്ത അറിവിടം**' എന്ന അധ്യായത്തിൽ പകർപ്പവകാശം, ക്രിയേറ്റീവ് കോമൺസ് ലൈസൻസ്, ഡിജിറ്റൽ ഉള്ളടക്കത്തിന്റെ ന്യായമായ ഉപയോഗം (Fair Use), സുരക്ഷിതമായ ഇന്റർനെറ്റ് ഉപയോഗം തുടങ്ങിയവ പ്രതിപാദിച്ചിട്ടുണ്ട്.

4. ഒൻപതാം ക്ലാസിലെ '**നന്മയുടെ വലക്കണ്ണികൾ**' എന്ന പാഠഭാഗത്ത് സോഷ്യൽമീഡിയ സൂക്ഷ്മതയോടെ എങ്ങനെ ഉപയോഗിക്കാം, ലോഗിൻവിവരങ്ങളും പാസ്‌വേഡും സുരക്ഷിതമാക്കേണ്ടതെങ്ങനെയെന്നും സൈബർകുറ്റകൃത്യങ്ങൾ, ഫാക്ട്ചെക്കിങ്ങിന്റെ ആവശ്യകത, ജാഗ്രതയോടെയുള്ള ഇന്റർനെറ്റ് ഉപയോഗം എന്നിവ വിശദമാക്കിയിട്ടുണ്ട്.

5. പത്താം ക്ലാസിലെ '**സൈബർ പ്രപഞ്ചം**' എന്ന അധ്യായത്തിൽ സൈബറിടത്തിൽ വിവരങ്ങൾ എങ്ങനെ ഉപയോഗിക്കണം, രചനാമോഷണം (Plagiarism), സ്പോയിലർ അലർട്ട് (Spoiler Alert) എന്നിങ്ങനെയുള്ള സൈബർലോകത്തെ ശരി-തെറ്റുകളെക്കുറിച്ചും സൈബർലോകത്തെ വിശ്വസനീയവും ആധികാരികവുമായ അറിവിന്റെ ഉറവിടങ്ങളെ സംബന്ധിച്ചും (Authentic Source of Information), സൈബർമര്യാദകൾ, ഡിജിറ്റൽ ഗാഡ്ജറ്റുകൾ അമിതമായി ഉപയോഗിക്കുന്നതു കൊണ്ടുള്ള അപകടങ്ങൾ തുടങ്ങിയവയും വിവരിച്ചിട്ടുണ്ട്.

4. ഐ.സി.ടി മാർഗനിർദേശങ്ങൾ അടങ്ങുന്ന സർക്കാർ ഉത്തരവ്

വിദ്യാഭ്യാസ രംഗത്ത് ഐ.സി.ടി. സാധ്യതകൾ ഉപയോഗിക്കുന്നതുമായി ബന്ധപ്പെട്ട 30.01.2023 ലെ സർക്കാർ ഉത്തരവു പ്രകാരം താഴെ പറയുന്ന മാർഗനിർദേശങ്ങൾ (പ്രധാനമായും സൈബർ സുരക്ഷയുമായി ബന്ധപ്പെട്ട്) സർക്കാർ പുറപ്പെടുവിച്ചിട്ടുണ്ട്.

1. "എസ്.സി.ഇ.ആർ.ടി.യും കൈറ്റും സംയുക്തമായി അംഗീകരിച്ചശേഷം മാത്രമേ സ്കൂളുകളിലേക്ക് ഡിജിറ്റൽ ഉള്ളടക്കം, ഡിജിറ്റൽ ലൈബ്രറികൾ തുടങ്ങിയ അക്കാദമിക് കണ്ടന്റ് ലഭ്യമാക്കാവൂ. പ്രൊപ്രൈറ്ററി ആയതും ലൈസൻസ് നിബന്ധനകൾ ഉള്ളതും ആയ സോഫ്റ്റ്വെയറുകൾ സ്കൂളുകളിൽ യാതൊരു കാരണവശാലും വിന്യസിക്കാൻ പാടില്ല".

2. "സ്കൂളുകൾക്കായി പുറപ്പെടുവിച്ചിട്ടുള്ള സൈബർ സേഫ്റ്റി പ്രോട്ടോക്കോൾ കൃത്യമായി പാലിക്കേണ്ടതാണ്. കുട്ടികളുടെ സ്വകാര്യവിവരങ്ങൾ പങ്കുവെക്കുന്ന തരത്തിലും മറ്റും സ്വകാര്യ സെർവറുകളിൽ ഹോസ്റ്റ് ചെയ്യുന്നതുൾപ്പടെയുള്ള പ്രവർത്തനങ്ങൾ സ്കൂൾ തലത്തിൽ നടത്താൻ പാടില്ല. പൊതുവിദ്യാഭ്യാസവകുപ്പ് അംഗീകരിച്ചതല്ലാത്ത ഇ-ഗവർണൻസ് ആപ്ലിക്കേഷനുകൾ

സവിശേഷ ഐ.ടി. പ്രവർത്തനങ്ങൾ എന്നിവയ്ക്കായി വകുപ്പിന്റെ പ്രത്യേകാനുമതി വാങ്ങേണ്ടതാണ്".

5. പ്രോട്ടോക്കോളിന്റെ പരിധിയും ഗുണഭോക്താക്കളും

സാങ്കേതികവിദ്യയുടെ അതിപ്രസരമുള്ള ഈ കാലഘട്ടത്തിൽ, പ്രത്യേകിച്ച് എ.ഐ. ഉപയോഗിച്ചുള്ള പുതിയ തരം ചതിക്കുഴികൾ വർധിച്ചുവരുന്ന സാഹചര്യത്തിൽ, വിദ്യാലയങ്ങളുമായി ബന്ധപ്പെട്ട എല്ലാ ഡിജിറ്റൽ ഇടപാടുകളും സുരക്ഷിതമാക്കാൻ ഈ മാർഗരേഖ സഹായിക്കുന്നു. ഐ.ടി. ആക്ട് (IT Act 2000), ഡിജിറ്റൽ വ്യക്തിഗത വിവരസംരക്ഷണ നിയമം (DPDP Act 2023), ഐ.ടി. ചട്ട ഭേദഗതി (2026) തുടങ്ങിയവയനുസരിച്ചുള്ള നിയമപരമായ സുരക്ഷാ മാനദണ്ഡങ്ങൾ ഇതിൽ ഉൾച്ചേർത്തിരിക്കുന്നു. കേരളത്തിൽ പൊതുവിദ്യാഭ്യാസ സംരക്ഷണ യജ്ഞത്തിന്റെയും മറ്റും ഭാഗമായി വിദ്യാലയങ്ങളിൽ സജ്ജീകരിച്ചിരിക്കുന്ന ഡിജിറ്റൽ ഉപകരണങ്ങളുടെയും നെറ്റ്‌വർക്കുകളുടെയും സുരക്ഷ ഉറപ്പാക്കുന്നതോടൊപ്പം ഈ പ്രോട്ടോക്കോൾ താഴെ പറയുന്ന വിഭാഗങ്ങളിലുള്ളവർക്കും മേഖലകൾക്കും പ്രയോജനപ്പെടുത്താവുന്നതാണ്.

1. ഗുണഭോക്താക്കൾ (Target Group)

1. കുട്ടികൾ: പ്രൈമറി മുതൽ ഹയർ സെക്കൻഡറി തലംവരെ പഠനം നടത്തുന്ന എല്ലാ കുട്ടികൾക്കും.
2. രക്ഷിതാക്കൾ: കുട്ടികളുടെ ഓൺലൈൻ പ്രവർത്തനങ്ങൾ നിരീക്ഷിക്കുകയും അവർക്ക് സുരക്ഷാ കവചമൊരുക്കുകയും ചെയ്യുന്ന എല്ലാ വ്യക്തികളും.
3. അധ്യാപകരും അനധ്യാപകരും: ബോധനപ്രവർത്തനങ്ങളിലും ഭരണപരമായ കാര്യങ്ങളിലും ഡിജിറ്റൽ സംവിധാനങ്ങൾ സുരക്ഷിതമായി ഉപയോഗിക്കുന്നവർ.

2. പ്രവർത്തന മേഖലകൾ (Applicable Areas)

1. അക്കാദമിക പ്രവർത്തനങ്ങൾ : ഡിജിറ്റൽ ക്ലാസ്മുറികൾ, ഡിജിറ്റൽ ഉള്ളടക്കം, പാഠപുസ്തകങ്ങളിലെ QR കോഡുകൾ, ഓൺലൈൻ പരിശീലനങ്ങൾ, പരീക്ഷകൾ തുടങ്ങിയവ.
2. ആർട്ടിഫിഷ്യൽ ഇന്റലിജൻസിന്റെ ഉപയോഗം: എ.ഐ. ടൂളുകൾ പഠനത്തിനും പരിശീലനത്തിനും ഉപയോഗിക്കുന്നത്.
3. ഭരണപരമായ ഡാറ്റ കൈകാര്യം ചെയ്യൽ : സമ്പൂർണ്ണ, സഹിതം, സമഗ്ര പ്ലസ് പോലെയുള്ള പോർട്ടലുകളിൽ ശേഖരിക്കുന്ന വിദ്യാർഥികളുടെയും അധ്യാപകരുടെയും വ്യക്തിഗത വിവരങ്ങൾ, അക്കാദമിക റിക്കോർഡുകൾ.
4. നെറ്റ്‌വർക്ക് & ഐ.ടി. സംവിധാനം : സ്കൂളിലെ കെ-ഫോൺ (K-FON) ഉൾപ്പെടെയുള്ള ഇന്റർനെറ്റ് കണക്ഷനുകൾ, ലാപ്ടോപ്പുകൾ, കമ്പ്യൂട്ടറുകൾ.
5. സ്കൂളിലെ സാമ്പത്തിക ഇടപാടുകൾ : സ്കോളർഷിപ്പുകൾ, യൂണിഫോം അലവൻസുകൾ തുടങ്ങിയവയ്ക്കായി വിദ്യാർഥികളുടെ ആധാർ, ബാങ്ക് അക്കൗണ്ട് വിവരങ്ങൾ തുടങ്ങിയവ ശേഖരിക്കൽ, ഓൺലൈൻ പണമിടപാടുകൾ നടത്തൽ.
6. വിദ്യാർഥി-അധ്യാപക ആശയവിനിമയം : മെസേജിങ് ഗ്രൂപ്പുകൾ (വാട്സാപ്പ് പോലെയുള്ള), ഇ-മെയിൽ, ലേണിംഗ് മാനേജ്മെന്റ് സിസ്റ്റങ്ങൾ (LMS), ഔദ്യോഗിക പ്ലാറ്റ്ഫോമുകളുടെ ഉപയോഗം.

7. സോഷ്യൽമീഡിയ ഉപയോഗം: സോഷ്യൽമീഡിയയിൽ സ്വന്തം ചിത്രങ്ങളും ലൊക്കേഷനും പങ്കുവെക്കുമ്പോൾ പുലർത്തേണ്ട ജാഗ്രതയെക്കുറിച്ചും, സൈബർ ആക്രമണങ്ങൾ റിപ്പോർട്ട് ചെയ്യുന്നതിനെ കുറിച്ചും.

8. ഓൺലൈൻ പഠന പരിസരം: സ്കൂളിലും സ്കൂളിനു പുറത്തും കുട്ടികൾ ഇന്റർനെറ്റും ഡിജിറ്റൽ ഉപകരണങ്ങളും ഉപയോഗിക്കുന്നതും സ്ക്രീൻ ടൈം നിയന്ത്രിക്കലും.

9. വിദ്യാർഥി പരിശീലനങ്ങൾ: ലിറ്റിൽ കൈറ്റ്സ് ഐ.ടി. ക്ലബ്ബുകൾ വഴിയും മറ്റും എല്ലാ വിദ്യാർഥികൾക്കും പ്രായോഗിക പരിശീലനം നൽകുന്നത്.

സൈബർ സേഫ്റ്റി പ്രോട്ടോക്കോൾ സ്കൂളിൽ നടപ്പാക്കുന്നതിനായി കുട്ടികളും അധ്യാപകരും രക്ഷിതാക്കളും ഒരുപോലെ പരിശ്രമിക്കേണ്ടതുണ്ട്. ഇതിനായി ഓരോരുത്തരും ശ്രദ്ധിക്കേണ്ട കാര്യങ്ങൾ താഴെ നൽകിയിരിക്കുന്നു.

6. സ്ഥാപനമേധാവി ഉറപ്പുവരുത്തേണ്ട കാര്യങ്ങൾ

1. സ.ഉ.(സ്വാധാ) നം. 165/2018/പൊ.വി.വ. തീയതി 10.01.2018, സ.ഉ.(സ്വാധാ) നം. 2177/2019/പൊ.വി.വ. തീയതി 06.06.2019 എന്നീ സർക്കാർ ഉത്തരവുകൾ പ്രകാരം സ്കൂളുകളും കൈറ്റും തമ്മിൽ ഒപ്പുവെച്ച പ്രത്യേക ധാരണാപത്രം അനുസരിച്ച് വിദ്യാലയങ്ങളിൽ ലഭ്യമാക്കിയിട്ടുള്ള ഇന്റർനെറ്റ് സംവിധാനം തടസ്സം കൂടാതെ സ്കൂൾ പ്രവൃത്തിസമയത്ത് വിദ്യാഭ്യാസ ആവശ്യങ്ങൾക്കായി എല്ലാ കുട്ടികൾക്കും ലഭ്യമാക്കുക എന്നത് സ്ഥാപന മേധാവിയുടെ ഉത്തരവാദിത്തമാണ്.

2. കുട്ടികളുടെ ഇന്റർനെറ്റ് ഉപയോഗം അധ്യാപകരുടെ നിരീക്ഷണത്തിലായിരിക്കണം. ഇന്റർനെറ്റ് ലഭ്യമാക്കുന്ന സ്ഥലങ്ങളിലും ലാബുകളിലും ഇരിപ്പിടം അതിനനുസൃതമായി ക്രമീകരിക്കേണ്ടതാണ്.

3. സ്കൂളിലെ Wi-Fi നെറ്റ്വർക്കിന് ശക്തവും സുരക്ഷിതവുമായ പാസ്വേഡുകൾ നൽകുകയും മറ്റുള്ളവർക്ക് Guest Wi-Fi സംവിധാനം ഏർപ്പെടുത്തുകയും ചെയ്യുക.

4. ആവശ്യമുള്ള സമയങ്ങളിൽ മാത്രമാണ് ലാബുകളിലും ക്ലാസുകളിലും ഇന്റർനെറ്റ് ഉപയോഗിക്കുന്നത് എന്ന കാര്യം ഉറപ്പുവരുത്തേണ്ടതാണ്. വിദ്യാലയ പ്രവൃത്തിസമയങ്ങൾക്കുപരിയായി ഇന്റർനെറ്റ് സംവിധാനം ഉപയോഗിക്കേണ്ടിവന്നാൽ സ്കൂൾ അധികൃതരുടെ അറിവും അനുവാദവും ഉറപ്പുവരുത്തേണ്ടതാണ്. ഇന്റർനെറ്റ് ഉപയോഗശേഷം കൃത്യമായി ഇന്റർനെറ്റ് സ്വിച്ച് ഓഫ് ചെയ്ത് കമ്പ്യൂട്ടർ ഷട്ട്ഡൗൺ ചെയ്തുവെന്ന് അനുമതി നൽകുന്നവർ ഉറപ്പുവരുത്തേണ്ടതാണ്.

5. ഇന്റർനെറ്റ് ശരിയായി ഉപയോഗിക്കുന്നത് സംബന്ധിച്ച മാർഗനിർദേശങ്ങൾ ക്ലാസുകളിലും ലാബുകളിലും പ്രദർശിപ്പിക്കാവുന്നതാണ്.

6. ആമുഖത്തിൽ സൂചിപ്പിച്ചതും ഐ.സി.ടി പാഠപുസ്തകങ്ങളിൽ സൈബർ സുരക്ഷയുമായി ബന്ധപ്പെട്ട് നൽകിയതുമായ കാര്യങ്ങൾ പ്രത്യേകം ചർച്ച ചെയ്യാൻ സ്കൂളുകളിൽ സംവിധാനം ഒരുക്കാവുന്നതാണ്.

7. സ്കൂളിൽ CCTV സംവിധാനം ഉപയോഗിക്കുമ്പോൾ താഴെ പറയുന്ന കാര്യങ്ങൾ ശ്രദ്ധിക്കുക.

   (a) സ്കൂളുകളിൽ സ്ഥാപിച്ചിട്ടുള്ള സി.സി.ടി.വി. (CCTV) കാമറകളിൽനിന്നുള്ള ദൃശ്യങ്ങൾ സ്കൂളിൽ തന്നെയുള്ള ഡി.വി.ആർ / എൻ.വി.ആർ (DVR/NVR) സംവിധാനത്തിൽ സുരക്ഷിതമായി സൂക്ഷിക്കേണ്ടതാണ്. യാതൊരു കാരണവശാലും സ്വകാര്യ വ്യക്തികളുടെയോ മറ്റ്

അനധികൃത ഏജൻസികളുടെയോ ക്ലൗഡ് സ്റ്റോറേജ് (Cloud Storage) സേവനങ്ങളിൽ ദൃശ്യങ്ങൾ ശേഖരിക്കുവാൻ പാടുള്ളതല്ല.

(b) കുട്ടികളുടെ സ്വകാര്യത ഹനിക്കാനിടയാക്കുമെന്നതിനാൽ സ്വകാര്യ സർവറുകൾ ഉൾപ്പെടെ പ്രയോജനപ്പെടുത്തി ക്ലാസ്മുറികൾക്ക് അകത്ത് CCTV ഉപയോഗിക്കുന്നത് ഒഴിവാക്കേണ്ടതാണ്. പരീക്ഷ പോലുള്ള പ്രത്യേക അവസരങ്ങളിൽ ഇതു ബാധകമല്ല. കാമറ സ്ഥാപിച്ച ഇടങ്ങളിൽ "നിങ്ങൾ CCTV നിരീക്ഷണത്തിലാണ്" എന്ന ബോർഡ് വ്യക്തമായി പ്രദർശിപ്പിക്കണം. സ്കൂളിൽ CCTV ഉപയോഗിക്കുമ്പോൾ അതാതു സമയങ്ങളിൽ സർക്കാരുകൾ നിർദേശിക്കുന്ന ചട്ടങ്ങൾ കൃത്യമായി പാലിക്കേണ്ടതാണ്.

8. സ്ഥാപനവുമായി ബന്ധപ്പെട്ട സോഷ്യൽമീഡിയ ആക്റ്റിവിറ്റികൾ സ്ഥാപന മേധാവി മോണിറ്റർ ചെയ്യേണ്ടതും ഇത് കുട്ടികളുടെ സ്വകാര്യത, ഡാറ്റസുരക്ഷിതത്വം തുടങ്ങിയവ പാലിക്കുന്നുണ്ടെന്ന് ഉറപ്പുവരുത്തേണ്ടതുമാണ്.

9. വിദ്യാലയത്തിൽ ശേഖരിക്കപ്പെടുന്ന ഡാറ്റയുടെ സ്വകാര്യതയും സുരക്ഷിതത്വവും പ്രധാനമാണ്. അതിനാൽ കുട്ടികളിൽനിന്നോ മറ്റുള്ളവരിൽനിന്നോ സർക്കാരിൽനിന്നോ ശേഖരിക്കുന്ന വിവരങ്ങൾ അനുമതി കൂടാതെ മറ്റുള്ളവർക്ക് കൈമാറരുത്.

10. ഈ ഡോക്യുമെന്റിലെ ഭാഗം 4ൽ പാമർശിച്ച സർക്കാർ ഉത്തരവിൽ പറഞ്ഞ മാർഗനിർദേശങ്ങൾ (ഡിജിറ്റൽ ഉള്ളടക്കം, സ്വതന്ത്ര സോഫ്റ്റ്വെയർ ഉപയോഗം തുടങ്ങിയവ) നിർബന്ധമായും പാലിക്കേണ്ടതാണ്.

11. അക്കാദമിക ഇന്നൊവേഷനുകൾ എന്ന നിലയിൽ നൂതനമായ സാങ്കേതികവിദ്യകൾ, സംവിധാനങ്ങൾ മുതലായവ സ്കൂളുകളിൽ ഉപയോഗിക്കുന്നതിനുമുമ്പ് അവ നിലവിലുള്ള വിദ്യാഭ്യാസ നയങ്ങൾ കാഴ്ചപ്പാടുകൾ തുടങ്ങിയവയ്ക്ക് അനുസൃതമാണ് എന്ന് ഉറപ്പുവരുത്തേണ്ടതും മേലധികാരികളിൽനിന്നും മുൻകൂർ അനുമതി വാങ്ങേണ്ടതുമാണ്.

12. കുട്ടികളുടെ ആധാർ വിവരങ്ങൾ ഉപയോഗിക്കുമ്പോൾ അതുമായി ബന്ധപ്പെട്ട നിയമങ്ങൾ ക്കനുസൃതമായി സർക്കാർ പുറപ്പെടുവിക്കുന്ന നിർദേശങ്ങൾ കൃത്യമായി പാലിക്കേണ്ടതാണ്. ആധാർ വിവരങ്ങൾ യാതൊരു കാരണവശാലും Spreadsheet വഴിയോ മറ്റോ കൈമാറാൻ പാടില്ല.

13. വിവിധ സോഫ്റ്റ്വെയറുകൾ, ആപ്ലിക്കേഷനുകൾ മുതലായവ ഉപയോഗിക്കുന്നതിനുള്ള പാസ്വേഡുകൾ അതിന്റെ ചുമതലയുള്ളവർക്കുമാത്രം ലഭ്യമാക്കുന്നതിന് ക്രമീകരണം ഒരുക്കേണ്ടതാണ്. ഔദ്യോഗിക പാസ്വേഡുകൾ Autosave ചെയ്യുന്നത് ഒഴിവാക്കണം.

14. സൈബർ സുരക്ഷയുമായി ബന്ധപ്പെട്ട കാര്യങ്ങൾ കൈകാര്യം ചെയ്യുന്നതിനായി, സ്ഥാപന മേലധികാരി, സ്റ്റാഫ് പ്രതിനിധികൾ, രക്ഷാകർത്തൃ പ്രതിനിധി, വിദ്യാർഥി പ്രതിനിധി തുടങ്ങിയവർ ഉൾപ്പെടുന്ന സ്കൂൾ സൈബർസുരക്ഷാസമിതി രൂപീകരിക്കാവുന്നതും സൈബർ സേഫ്റ്റി കോഡിനേറ്റർ/ കോഡിനേറ്റർമാർ എന്ന നിലയിൽ അധ്യാപകർക്ക് ചുമതല നൽകാവുന്നതുമാണ്. സ്കൂൾ ഐ.ടി കോഡിനേറ്റർ, കൈറ്റ് മെന്റർ എന്നിവരെയും ആവശ്യമെങ്കിൽ ഇതിനായി പരിഗണിക്കാം.

15. സൈബർ സുരക്ഷയുമായി ബന്ധപ്പെട്ട കാര്യങ്ങൾ റിപ്പോർട്ട് ചെയ്യുന്നതിനുള്ള സംവിധാനം എല്ലാ സ്കൂളിലും ഒരുക്കാവുന്നതാണ്. സൈബർ സേഫ്റ്റി കോഡിനേറ്ററെ ഈ ചുമതല ഏൽപ്പിക്കാവുന്നതാണ്. റിപ്പോർട്ടിംഗ് ഓഫീസറെ കുറിച്ചുള്ള വിവരങ്ങൾ സ്കൂളിൽ പ്രദർശിപ്പിക്കാവുന്നതാണ്.

16. ഔദ്യോഗിക സീലിന് തുല്യമായ ഡിജിറ്റൽ സിഗ്നേച്ചർ ടോക്കണും അതിന്റെ പാസ്‌വേഡും സ്വന്തം കൈവശം രഹസ്യമായി സൂക്ഷിക്കുക. സുരക്ഷാ ഭീഷണി മുൻനിർത്തി സൈബർ കഫേകളിലും പൊതു ഇടങ്ങളിലും ഇത് ഉപയോഗിക്കുകയോ കൈമാറുകയോ ചെയ്യരുത്. ഉപയോഗശേഷം പോർട്ടലിൽനിന്ന് ലോഗൗട്ട് ചെയ്ത് ടോക്കൺ നീക്കം ചെയ്യേണ്ടതും SPARK, BiMS തുടങ്ങിയ ഔദ്യോഗിക പോർട്ടലുകളുടെ ലോഗിൻ വിവരങ്ങൾ അതത് ഉദ്യോഗസ്ഥർ മാത്രം കൈകാര്യം ചെയ്യേണ്ടതുമാണ്.

17. സ്കൂളുകളിൽ വർഷത്തിൽ ഒരുതവണയെങ്കിലും 'സൈബർ സേഫ്റ്റി ഓഡിറ്റ്' നടത്താവുന്നതാണ്. (ഇതിനായുള്ള മാർഗനിർദേശങ്ങൾ പ്രത്യേകം ലഭ്യമാക്കുന്നതാണ്.)

7. അധ്യാപകർ ഉറപ്പുവരുത്തേണ്ടത്.

1. ക്ലാസിൽ ഇന്റർനെറ്റ് നേരിട്ട് ഉപയോഗിക്കുന്നത് ഒഴിവാക്കേണ്ടതാണ്. ആവശ്യമായ വിഭവങ്ങൾ മുൻകൂട്ടി ശേഖരിച്ച് മാത്രം ക്ലാസ്മുറിയിൽ ഉപയോഗിക്കേണ്ടതാണ്. എന്നാൽ, വിദ്യാഭ്യാസവകുപ്പ് തയ്യാറാക്കിയ പോർട്ടലുകളിൽ ലഭ്യമാക്കിയിട്ടുള്ള വിഭവങ്ങൾ ക്ലാസിൽ നേരിട്ട് ഉപയോഗിക്കാവുന്നതാണ്.

2. അധ്യാപകരുടേയോ മറ്റ് ചുമതലയുള്ളവരുടെയോ മേൽനോട്ടത്തിൽ മാത്രം കുട്ടികൾക്ക് ഇന്റർനെറ്റ് ഉപയോഗിക്കാൻ അവസരം നൽകേണ്ടതാണ്.

3. സ്കൂളിലെ ഇന്റർനെറ്റ് ഉപയോഗം പഠനാവശ്യങ്ങൾക്കും ഔദ്യോഗിക ആവശ്യങ്ങൾക്കും മറ്റു പഠനാനുബന്ധ പ്രവർത്തനങ്ങൾക്കും മാത്രമായി പരിമിതപ്പെടുത്തേണ്ടതാണ്.

4. ഇന്റർനെറ്റ് അധിഷ്ഠിതമായ പ്രവർത്തനങ്ങൾ ക്ലാസ് ഗ്രൂപ്പുകളിൽ നൽകുമ്പോൾ പ്രവർത്തനങ്ങൾ മുൻകൂട്ടി ആസൂത്രണം ചെയ്യുകയും കുട്ടികൾ ആ പ്രവർത്തനങ്ങൾവിട്ട് മറ്റുള്ളവയിലേക്ക് പോകുന്നതിനുള്ള അവസരങ്ങൾ ഉണ്ടാകാതെ നോക്കുകയും വേണം.

5. ഇന്റർനെറ്റിൽനിന്നും ശേഖരിക്കുന്നതും എ.ഐ. സങ്കേതങ്ങൾ ഉപയോഗിച്ച് തയ്യാറാക്കുന്നതുമായ വിഭവങ്ങളുടെ ആധികാരികത ഉറപ്പുവരുത്തി മാത്രമേ അക്കാദമിക പ്രവർത്തനങ്ങൾക്ക് ഉപയോഗിക്കാവൂ.

6. നിർമ്മിതബുദ്ധി ഉപയോഗപ്പെടുത്തി നിർമ്മിക്കുന്ന റിസോഴ്സുകളോടൊപ്പം (സിന്തറ്റിക്കലി ജനറേറ്റഡ് ഇൻഫർമേഷൻ) അവലംബം രേഖപ്പെടുത്തണം. മറ്റ് ഉറവിടങ്ങളിൽ നിന്നുള്ള ഏതൊരു റിസോഴ്സ് ഉപയോഗിക്കുമ്പോഴും അവലംബം നൽകണം.

7. വിവിധ സോഫ്റ്റ്വെയറുകൾ, ആപ്ലിക്കേഷനുകൾ മുതലായവ ഉപയോഗിക്കുന്നതിനുള്ള പാസ്‌വേഡുകൾ സുരക്ഷിതമായി കൈകാര്യം ചെയ്യേണ്ടതാണ്.

8. സ്വകാര്യത, ഡാറ്റാ പ്രൈവസി എന്നിവ ഹനിക്കുന്നതരത്തിൽ കുട്ടികളുടെ ഡാറ്റകൾ കൈകാര്യം ചെയ്യരുത്. കുട്ടികളുമായി ബന്ധപ്പെട്ട സെൻസിറ്റീവ് വിവരങ്ങൾ ശേഖരിക്കുന്നതിന് സോഷ്യൽമീഡിയ ഉപയോഗിക്കരുത്.

9. കുട്ടികൾക്കുള്ള ക്ലാസ്റും/ഐ.ടി. പ്രവർത്തനങ്ങൾ സ്കൂളിൽവച്ചുതന്നെ ചെയ്തു തീർക്കാൻ അവസരം നൽകേണ്ടതാണ്. ഡിജിറ്റൽ വിഭജനം ഇല്ലാത്ത വിധം എല്ലാ കുട്ടികൾക്കും തുല്യത ഉറപ്പാക്കണം. ഹോം അസൈൻമെന്റുകൾക്ക് ഡിജിറ്റൽ ഉപകരണങ്ങളുടെ ലഭ്യത അവശ്യമായി വരരുത്. എന്നാൽ, രക്ഷാകർത്താക്കൾക്കായി സമ്പൂർണ പ്ലസ്, സഹിതം തുടങ്ങിയ ഓൺലൈൻ സൗകര്യങ്ങൾ നൽകാം. കുട്ടികൾക്ക് 'കീ ടു എൻടൻസ്' പോലുള്ള പരിപാടികളിൽ പങ്കെടുക്കുന്നതിന് വീട്ടിൽ സംവിധാനമില്ലെങ്കിൽ അത് സ്കൂളിലോ മറ്റോ ഏർപ്പെടുത്താവുന്നതാണ്.

8. വിദ്യാർഥികൾ ശ്രദ്ധിക്കേണ്ട കാര്യങ്ങൾ

1. വിദ്യാലയങ്ങളിലെ ഇന്റർനെറ്റ് ഉപയോഗം അധ്യാപകരുടെ നിർദേശാനുസരണം മാത്രമായിരിക്കണം.

2. വിശ്വസിക്കാൻ പ്രയാസമുള്ള ഓഫറുകളോ സംശയാസ്പദമായ ലിങ്കുകളോ (ആകർഷകമായ ഓഫറുകൾ നൽകുന്നവയോ വലിയ സമ്മാനങ്ങൾ ലഭിച്ചു എന്ന രീതിയിലുള്ള സന്ദേശങ്ങളോ) വന്നാൽ അവയിൽ ക്ലിക്ക് ചെയ്യുകയോ പ്രതികരിക്കുകയോ ചെയ്യരുത്.

3. പുതിയ ഗെയിമുകളോ സോഷ്യൽമീഡിയ ആപ്പുകളോ ഡൗൺലോഡ് ചെയ്യുന്നതിനു മുമ്പ്, അവ ഉപയോഗിക്കേണ്ട പ്രായപരിധിയും (Age Rating) ഡാറ്റാ പെർമിഷനുകളും (Data Permissions) ഒരുമിച്ച് പരിശോധിച്ച് നിങ്ങൾക്ക് അനുയോജ്യമാണെന്ന് ഉറപ്പുവരുത്തുക.

4. ഗെയിമുകളിലെ സൗജന്യ ഓഫറുകൾ, ലിമിറ്റഡ് ടൈം ഡീലുകൾ, അല്ലെങ്കിൽ പെട്ടെന്ന് ലെവൽ മാറാനുള്ള പ്രലോഭനങ്ങൾ എന്നിവ അനാവശ്യമായി പണം ചെലവാക്കിക്കാൻ ഡിസൈൻ ചെയ്തിട്ടുള്ള 'ഡാർക്ക് പാറ്റേണുകൾ' (Dark Patterns) ആകാൻ സാധ്യതയുള്ളതിനാൽ ജാഗ്രത പാലിക്കുക.

5. വിശ്വസനീയമല്ലാത്ത ഉറവിടങ്ങളിൽനിന്നോ വെബ്സൈറ്റുകളിൽനിന്നോ ലഭിക്കുന്ന ആപ്ലിക്കേഷനുകൾ ഡൗൺലോഡ് ചെയ്യുകയോ, ഇൻസ്റ്റാൾ ചെയ്ത് ഉപയോഗിക്കുകയോ ചെയ്യരുത്.

6. ഓൺലൈൻ ഗെയിമുകൾക്ക് നിയന്ത്രണം പാലിക്കുക. അപരിചിതർ നൽകുന്ന ചാലഞ്ച്, സ്വകാര്യവിവരങ്ങളും ചിത്രങ്ങളും കൈമാറാനുള്ള ആവശ്യങ്ങൾ എന്നിവയിൽ യാതൊരു കാരണവശാലും അകപ്പെടാതിരിക്കാൻ പ്രത്യേകം ശ്രദ്ധിക്കുക. ഓൺലൈൻ ഗെയിമുകളിൽ കാമറ പെർമിഷൻ, ലൈവ് ചാറ്റ് എന്നിവ ഒഴിവാക്കുക.

7. ലൊക്കേഷൻ തിരിച്ചറിയാൻ സാധിക്കുന്ന തരത്തിൽ 'ലൈവ് ലൊക്കേഷനോ' ചിത്രങ്ങളോ ഒരിക്കലും സമൂഹ മാധ്യമങ്ങളിൽ പങ്കുവെക്കരുത്. മൊബൈൽ നമ്പർ ഉൾപ്പെടെയുള്ള സെൻസിറ്റീവ് വിവരങ്ങളും പങ്കുവയ്ക്കരുത്.

8. നഗ്നത പ്രദർശിപ്പിക്കുന്ന തരത്തിലുള്ള ചിത്രങ്ങളോ വീഡിയോകളോ പകർത്തുകയോ പങ്കുവെക്കുകയോ ചെയ്യരുത്. ഇത് പിന്നീട് ബ്ലാക്ക്മെയിലിംഗിനും സൈബർ കെണികൾക്കും കാരണമായേക്കാം എന്നതിനാൽ അതീവ ജാഗ്രത പാലിക്കുക. ഇന്റർനെറ്റിൽ ഒരിക്കൽ പങ്കുവെക്കുന്ന ചിത്രം പിന്നീട് പൂർണ്ണമായും മായ്ച്ചു കളയുക അസാധ്യമാണ്.

9. ഓൺലൈൻ അക്കൗണ്ടുകളുടെ പാസ്വേഡുകൾ ആരുമായും പങ്കുവെക്കരുത്. ഓരോ അക്കൗണ്ടിനും വ്യത്യസ്തവും ശക്തവുമായ പാസ്വേഡുകൾ/പാസ് ഫ്രേസുകൾ ഉപയോഗിക്കുക.

10. ഓൺലൈനിലൂടെയും ആരെയും ഭീഷണിപ്പെടുത്തുകയോ പരിഹസിക്കുകയൊ ചെയ്യരുത്. ആരെങ്കിലും നിങ്ങളെ പരിഹസിക്കുകയോ ഭീഷണിപ്പെടുത്തുകയോ ചെയ്താൽ തിരിച്ച് പ്രതികരിക്കാതെ ഉടൻ തന്നെ അവരെ Block ചെയ്യുകയും ആ വിവരം മാതാപിതാക്കളോടോ അധ്യാപകരോടോ പറയുകയും ചെയ്യുക.

11. മോശമായ സന്ദേശങ്ങൾ, കമന്റുകൾ അല്ലെങ്കിൽ പോസ്റ്റുകൾ ശ്രദ്ധയിൽ പെട്ടാൽ അവയുടെ സ്ക്രീൻഷോട്ട് (Screenshot) എടുത്തുവയ്ക്കുക. പരാതി നൽകാൻ ഇത് അത്യാവശ്യമാണ്.

12. സ്കൂൾ പാഠ്യപദ്ധതിയുടെ ഭാഗമായുള്ള ഹോംവർക്കുകളിലോ പ്രോജക്ടുകളിലോ കൃത്രിമം കാണിക്കാൻ എ.ഐ. സാധ്യത ഉപയോഗിക്കുന്നതും നിയമപരമായ പ്രത്യാഘാതങ്ങൾ

മനസ്സിലാക്കാതെ വ്യാജമായ (Pirated) സിനിമകളോ സോഫ്റ്റ്വെയറുകളോ ഡൗൺലോഡ് ചെയ്യുന്നതും ഒഴിവാക്കി സാങ്കേതികവിദ്യയെ സത്യസന്ധമായും സുരക്ഷിതമായും ഉപയോഗിക്കാൻ ശ്രദ്ധിക്കുക.

13. എ.ഐ. സംവിധാനങ്ങളെ ആശയരൂപീകരണത്തിനുള്ള ഒരു സഹായി ആയി മാത്രം കാണുക. അതിനെ മാത്രം ആശ്രയിക്കരുത്. ഇതിൽനിന്നും ലഭിക്കുന്ന സഹായം ഉപയോഗിച്ച് സ്വന്തമായി ചിന്തിക്കാനും പ്രശ്നപരിഹാരം കണ്ടെത്താനുമുള്ള കഴിവ് വികസിപ്പിക്കുക.

14. എ.ഐ. നൽകുന്ന വസ്തുതകൾ മറ്റ് വിശ്വസനീയ സ്രോതസ്സുകളുമായി (പുസ്തകങ്ങൾ, അധ്യാപകർ, വിശ്വാസയോഗ്യമായ വെബ്സൈറ്റുകൾ) താരതമ്യം ചെയ്ത് ഉറപ്പുവരുത്തി മാത്രം ഉപയോഗിക്കുക.

15. വിദ്യാലയങ്ങൾ, ഓഫീസുകൾ തുടങ്ങി പൊതുഇടങ്ങളിൽ ഉപയോഗിക്കുന്ന കമ്പ്യൂട്ടറുകളിൽ വ്യക്തിഗത വിവരങ്ങളോ, ചിത്രങ്ങളോ സൂക്ഷിക്കരുത്. ചിത്രങ്ങൾ മോർഫ് ചെയ്തും മറ്റുമെല്ലാം ദുരുപയോഗം ചെയ്യപ്പെടാം. മറ്റുള്ള കുട്ടികളുടെ (വ്യക്തികളുടെ) വിവരങ്ങളും ഇപ്രകാരം ദുരുപയോഗം ചെയ്യരുത്.

16. പെൻഡ്രൈവുകളോ ഇതര സ്റ്റോറേജ് ഡിവൈസുകളോ അനുവാദം കൂടാതെ സ്കൂൾ കമ്പ്യൂട്ടറുകളിലോ പൊതുകമ്പ്യൂട്ടറുകളിലോ ഉപയോഗിക്കരുത്.

17. മൊബൈൽ ഫോൺ, ലാപ്ടോപ്പ്, പെൻഡ്രൈവ് തുടങ്ങിയ ഡിജിറ്റൽ ഉപകരണങ്ങൾ അപരിചിതരെ ഏൽപിക്കരുത്.

18. ഓൺലൈൻ പരിചയം മാത്രമുള്ളവരെ രക്ഷിതാക്കളുടെയോ മറ്റോ കൂടെയല്ലാതെ ഒരിക്കലും നേരിട്ട് കാണാൻ ശ്രമിക്കരുത്. പരിചയമില്ലാത്തതോ, വിശ്വാസമില്ലാത്തതോ ആയ ആളുകൾ അയയ്ക്കുന്ന ഇ-മെയിൽ ഉൾപ്പെടെയുള്ള സന്ദേശങ്ങൾ തുറക്കരുത്.

19. വസ്തുതാവിരുദ്ധവും, ഹാനികരവുമായ സന്ദേശങ്ങൾ, ചിത്രങ്ങൾ, വീഡിയോകൾ തുടങ്ങിയവ ഫോർവേർഡ് ചെയ്യുന്നത് സൈബർ നിയമപ്രകാരം കുറ്റകരമാണ് എന്നോർക്കുക.

20. സൈബർ ഉപയോഗവുമായി ബന്ധപ്പെട്ട് ഉണ്ടാകുന്ന ബുദ്ധിമുട്ടുകൾ, ഭീഷണികൾ തുടങ്ങിയവ രക്ഷിതാക്കളുമായും അധ്യാപകരുമായും തുറന്ന് സംസാരിക്കുക.

21. അനധികൃതമായി ആരെങ്കിലും നിങ്ങളുടെ ഫോട്ടോ എടുക്കുന്നതായി ശ്രദ്ധയിൽപെട്ടാൽ അധ്യാപകരേയോ രക്ഷിതാക്കളെയോ അറിയിക്കേണ്ടതാണ്.

22. എ.ഐ. ടൂളുകൾ ഉപയോഗിക്കുമ്പോൾ വിവരങ്ങളുടെ കൃത്യത പരിശോധിക്കാനും (Fact-checking) പക്ഷപാതങ്ങൾ (Bias) തിരിച്ചറിയാനും ശ്രദ്ധിക്കണം.

23. സമൂഹത്തിന്റെ വിവിധ മേഖലകളിൽ സൈബർ സേഫ്റ്റി പ്രോഗ്രാമുകൾ / അനുബന്ധ ക്വിസ്/ സെമിനാർ എന്നിവയിലൂടെ സൈബർ സുരക്ഷാ പ്രചാരണത്തിൽ പങ്കാളികളാവുക. ഐ.സി.ടി പാഠപുസ്തകങ്ങളിൽ ഉൾപ്പെടുത്തിയിട്ടുള്ള സൈബർ സുരക്ഷയുമായി ബന്ധപ്പെട്ട ഉള്ളടക്കങ്ങൾ വായിച്ചു മനസ്സിലാക്കി മറ്റുള്ളവരുമായി പങ്കിടാൻ ഇത്തരം സാഹചര്യങ്ങൾ ഉപയോഗിക്കുക.

24. കീ ടു എൻട്രൻസ്, ഓൺലൈൻ അപേക്ഷകൾ സമർപ്പിക്കൽ തുടങ്ങിയ കാര്യങ്ങൾക്കായി വീട്ടിൽ ഓൺലൈൻ സൗകര്യമില്ലെങ്കിൽ ആയത് സ്കൂളിലെ ലാബിൽ നിന്നും ചെയ്യാൻ സൗകര്യമൊരുക്കാൻ അധ്യാപകരോട് പറയേണ്ടതാണ്.

25. സൈബർ സ്പേസിൽ പ്രധാനമായും കുട്ടികളെ ലക്ഷ്യമിട്ടുകൊണ്ടുള്ള നിരവധി കുറ്റകൃത്യങ്ങൾ (സൈബർ ക്രൈമുകൾ) നടക്കുന്നുണ്ട്. അവയിൽ പ്രധാനപ്പെട്ടവ അനുബന്ധമായി (അനുബന്ധം 1) നൽകിയിട്ടുണ്ട്.

[ഇതിനു പുറമെ ഔദ്യോഗിക വെബ്സൈറ്റുകളിലും (https://cybercrime.gov.in/) സർക്കാർ പുറപ്പെടുവിക്കുന്ന ഇതുമായി ബന്ധപ്പെട്ട രേഖകളിലും കൂടുതൽ സൈബർ കുറ്റകൃത്യങ്ങൾ വിശദീകരിച്ചിട്ടുണ്ട്. ഇവ വായിച്ചു മനസ്സിലാക്കുക.]

9. രക്ഷിതാക്കൾ ശ്രദ്ധിക്കേണ്ട കാര്യങ്ങൾ

1. വിദ്യാലയങ്ങളിലെ ഉപയോഗത്തിന് സ്കൂൾ നിർദേശിക്കുന്നതല്ലാത്ത ഉപകരണങ്ങൾ കുട്ടിക്ക് നൽകരുത്.

2. കമ്പ്യൂട്ടർ, മൊബൈൽ ഫോൺ, ഇന്റർനെറ്റ് തുടങ്ങിയവ കുട്ടി ഉപയോഗിക്കുമ്പോൾ രക്ഷിതാക്കളുടെ പ്രത്യേക ശ്രദ്ധ ഉറപ്പുവരുത്തേണ്ടതാണ്.

3. പുതിയ സാങ്കേതികവിദ്യകളുടെ ഉപയോഗം മനസ്സിലാക്കാൻ ശ്രമിക്കുക. നിങ്ങളുടെ അറിവ് പുതുക്കിക്കൊണ്ടിരിക്കുക. സാമൂഹ്യമാധ്യമങ്ങളും മറ്റും ഉപയോഗിക്കുന്നതിനെക്കുറിച്ച് കുട്ടികളുമായി തുറന്ന് ചർച്ച ചെയ്യുക.

4. സാങ്കേതിക സംവിധാനങ്ങളുടെ (ഇന്റർനെറ്റ്, മൊബൈൽ ഫോൺ) അമിത ഉപയോഗം കുട്ടികളിലുണ്ടോ എന്ന് നിരീക്ഷിക്കുക. കുട്ടിയിൽ എന്തെങ്കിലും തരത്തിലുള്ള പെരുമാറ്റ വൈകല്യങ്ങളുടെ സൂചന കാണുകയോ സൈബർ കുറ്റകൃത്യങ്ങൾക്ക് അവർ ഇരയായെന്ന് അറിയുകയോ ചെയ്താൽ കുട്ടികളോട് തുറന്ന് സംസാരിക്കുക. കൂടുതൽ ഭയപ്പെടുത്താതെ കാര്യങ്ങൾ വിശദമായി ചോദിച്ചറിയുകയും ബന്ധപ്പെട്ട ഉദ്യോഗസ്ഥരോട് പരാതിപ്പെടുകയും ചെയ്യുക. ആവശ്യമെങ്കിൽ കൗൺസിലിംഗ് നൽകുക.

5. ഡിജിറ്റൽ അറസ്റ്റ് എന്ന പേരിൽ ഉൾപ്പെടെ നടക്കുന്ന നൂതന തട്ടിപ്പുകളെ കുറിച്ച് അറിവുണ്ടായിരിക്കുക.

6. സ്കൂളുകളിൽ ലിറ്റിൽ കൈറ്റ്സ് യൂണിറ്റുകൾ ഉൾപ്പെടെ സംഘടിപ്പിക്കുന്ന വിവിധ സൈബർ സുരക്ഷാ ബോധവൽക്കരണപരിപാടികളിൽ സ്ഥിരമായി പങ്കെടുക്കുക.

7. കുട്ടികൾക്ക് സുരക്ഷിതമായ ഇന്റർനെറ്റ് അനുഭവം ഉറപ്പാക്കുന്നതിന് ലാപ്ടോപ്പുകളോ മൊബൈൽ ഫോണോ നൽകുമ്പോൾ വെബ് ബ്രൗസറുകൾ നൽകുന്ന ഫിൽട്ടറുകളോ പോർട്ടലുകളിലെ ഫിൽട്ടറുകളോ പ്രവർത്തനക്ഷമമാക്കുക. ഇതിനുള്ള കാരണം കുട്ടിയുമായി പങ്കുവയ്ക്കുക.

8. കുട്ടികൾ ഓൺലൈനിൽ ആരുമായി ബന്ധപ്പെടുന്നു എന്നത് അതീവ ജാഗ്രത വേണ്ട കാര്യമാണ്, കാരണം ഇത്തരം സമ്പർക്കങ്ങളിലൂടെയാണ് ഓൺലൈൻ ഗ്രൂമിംഗിനും ചൂഷണങ്ങൾക്കുമുള്ള സാധ്യത ഏറ്റവും കൂടുതലായി കാണപ്പെടുന്നത്.

9. രക്ഷിതാക്കളുടെ ക്രെഡിറ്റ്/ഡെബിറ്റ് കാർഡിന്റെ പിൻ കോഡ്, പാസ്വേഡ്, ഓൺലൈൻ ബാങ്ക് അക്കൗണ്ട് പാസ്വേഡ് തുടങ്ങിയവ കുട്ടികളുമായി ഷെയർ ചെയ്യരുത്.

10. രക്ഷിതാക്കളുടെ സോഷ്യൽമീഡിയ അക്കൗണ്ടുകളോ ഇ-മെയിൽ അക്കൗണ്ടുകളോ കുട്ടികൾക്ക് ഉപയോഗിക്കാൻ നൽകരുത് .

11. സോഷ്യൽമീഡിയ പ്ലാറ്റ്ഫോമുകൾ ഉപയോഗിക്കാനുള്ള നിയമപരമായ പ്രായപരിധി കുട്ടികൾ പാലിക്കുന്നുണ്ടെന്ന് ഉറപ്പുവരുത്തുക. കുട്ടികളുടെ അക്കൗണ്ടുകൾ എപ്പോഴും

'Private' മോഡിലാക്കി വെക്കുക. ഇത് അപരിചിതർ അവരുടെ ഫോട്ടോകളോ വിവരങ്ങളോ കാണുന്നത് തടയാൻ സഹായിക്കും.

12. ഡിജിറ്റൽ ഫൂട്ട്പ്രിന്റ് (Digital Footprint) : ഒരിക്കൽ ഇന്റർനെറ്റിൽ പങ്കുവെക്കുന്ന കാര്യങ്ങൾ പൂർണ്ണമായും മായ്ച്ചു കളയൽ ശ്രമകരമാണെന്ന കാര്യം കുട്ടിയെ ബോധ്യപ്പെടുത്തുക. ഭാവിയിലെ പഠനത്തെയോ ജോലിയെയോ ബാധിക്കുന്ന ഒന്നും പോസ്റ്റ് ചെയ്യാതിരിക്കാൻ ശ്രദ്ധിക്കുക.

13. കുട്ടികൾ കമ്പ്യൂട്ടറിൽ/മൊബൈലിൽ ചെയ്യുന്ന പ്രവർത്തനങ്ങൾ മോണിറ്റർ ചെയ്യുന്നതിന്റെ ഭാഗമായി ഉപയോഗശേഷം ആപ്പുകളുടെ ബ്രൗസിങ്ങ് ഹിസ്റ്ററി പരിശോധിക്കുന്നത് നല്ലതായിരിക്കും. 'Family Center', 'Family Link' തുടങ്ങിയ സംവിധാനങ്ങൾ ഉപയോഗിക്കാം.

14. ഫോണിലെ 'ഇൻ-ആപ്പ് പർച്ചേസ്' (In-app purchases) ഓപ്ഷൻ ഡിസേബിൾ ചെയ്യുകയും സുരക്ഷിതമായ 'കിഡ്-സേഫ്' (Kid-Safe) ആപ്പുകൾ മാത്രം ഉപയോഗിക്കുകയും ചെയ്യുക.

15. സ്ക്രീൻ ടൈം (Screen Time): ഡിജിറ്റൽ ഉപകരണങ്ങളായ സ്മാർട്ട്ഫോൺ, കമ്പ്യൂട്ടർ, ടെലിവിഷൻ എന്നിവ ഉപയോഗിക്കുന്നതിനായി നാം ചെലവഴിക്കുന്ന സമയമാണ് സ്ക്രീൻ ടൈം. ഇത് അമിതമാകുന്നത് ശാരീരികവും മാനസികവുമായ ആരോഗ്യത്തെ ബാധിച്ചേക്കാം. നിങ്ങളുടെ ഫോണിലെ 'Digital Wellbeing' അല്ലെങ്കിൽ 'Screen Time' സെറ്റിംഗ്സ് ഉപയോഗിച്ച് ഓരോ ആപ്പിനും സമയപരിധി നിശ്ചയിക്കാവുന്നതാണ്.

16. കുട്ടികളുമായി സൗഹൃദപരമായ അന്തരീക്ഷം നിലനിർത്തുക. ഓൺലൈനിൽ എന്തെങ്കിലും ബുദ്ധിമുട്ടുകൾ നേരിട്ടാൽ (ഉദാഹരണത്തിന് സൈബർ ബുള്ളിയിംഗ്) പേടിക്കാതെ നിങ്ങളോട് പറയാനുള്ള ധൈര്യം അവർക്ക് നൽകുക. അവരെ സുരക്ഷിതമായ ഡിജിറ്റൽ ശീലങ്ങൾ പഠിപ്പിക്കുക.

10. പൊതുനിർദേശങ്ങൾ

1. എല്ലാ സോഷ്യൽമീഡിയ, ബാങ്കിംഗ് അക്കൗണ്ടുകളിലും ടു-ഫാക്ടർ ഓതന്റിക്കേഷൻ (2FA/MFA) എനേബിൾ ചെയ്യുക.

   ഡിജിറ്റൽ അക്കൗണ്ടുകൾക്ക് പാസ്വേഡിന് പുറമെ നൽകുന്ന രണ്ടാമതൊരു സുരക്ഷാ കവചമാണ് ടു-ഫാക്ടർ ഓതന്റിക്കേഷൻ അഥവാ 2FA. ഒരു അക്കൗണ്ട് തുറക്കാൻ ഒന്നിന് പകരം രണ്ട് തിരിച്ചറിയൽ രീതികൾ (Factors) ഉപയോഗിക്കുന്ന പ്രക്രിയയാണിത്. ഒരു പ്ലാറ്റ്ഫോമിലേയ്ക്ക് ലോഗിൻ ചെയ്യുമ്പോൾ നിങ്ങളുടെ മൊബൈൽ ഫോണിലേക്ക് വരുന്ന OTP (One Time Password), അല്ലെങ്കിൽ ഒരു സുരക്ഷാ കീ (Security Key) ഇതിന് ഉദാഹരണമാണ്.

2. റെയിൽവെ സ്റ്റേഷൻ, കഫേകൾ എന്നിവിടങ്ങളിലെ സൗജന്യ വൈഫൈ ഉപയോഗിച്ച് കഴിവതും ബാങ്ക് ഇടപാടുകൾ നടത്തരുത്.

3. വീടുകളിലെ വൈഫൈ റൂട്ടറുകൾക്ക് ശക്തമായ പാസ്വേഡ് നൽകുക.

4. വീഡിയോ കോളുകളിൽ സംസാരിക്കുന്നത് നിങ്ങളുടെ സുഹൃത്തോ ബന്ധുവോ ആണെന്ന് ഉറപ്പുവരുത്തുക. എ.ഐ. ഉപയോഗിച്ച് നിർമ്മിച്ച ഡീപ് ഫേക്ക് വീഡിയോ കോളുകൾ ആയിരിക്കാനും സാധ്യതയുണ്ട്. സംശയം തോന്നിയാൽ പ്രസ്തുത വ്യക്തിയെ മറ്റൊരു രീതിയിൽ (സാധാരണ ഫോൺ കോൾ വഴി) ബന്ധപ്പെട്ട് സംശയ നിവാരണം നടത്തുക.

5. സോഷ്യൽമീഡിയ മര്യാദകൾ (Netiquette): മറ്റൊരാളെ പരിഹസിക്കുന്നതോ അപകീർത്തിപ്പെടുത്തുന്നതോ ആയ പോസ്റ്റുകളോ കമന്റുകളോ പങ്കുവെക്കരുത്. ഇത് സൈബർ ബുള്ളിയിംഗ്

(Cyber Bullying) ആയി കണക്കാക്കപ്പെടും.

6. ഫോണിലെയും കമ്പ്യൂട്ടറിലെയും ഓപ്പറേറ്റിംഗ് സിസ്റ്റവും ആപ്പുകളും കൃത്യസമയത്ത് അപ്ഡേറ്റ് ചെയ്യുക. സുരക്ഷാ പിഴവുകൾ (Security Patches) പരിഹരിക്കാൻ ഇത് അത്യാവശ്യമാണ്.

7. സുരക്ഷിതമായ സ്രോതസ്സുകളിൽ (Play Store, App Store, etc) നിന്നു മാത്രം ആപ്പുകൾ ഡൗൺലോഡ് ചെയ്യുക. APK ഫയലുകൾ, ലിങ്കുകൾ തുടങ്ങിയവ വഴി ഇൻസ്റ്റാൾ ചെയ്യുന്നത് മാൽവെയർ (Malware) ആക്രമണങ്ങൾക്കും ഡാറ്റാ ചോർച്ചയ്ക്കും കാരണമാകും. ഇതല്ലാത്ത തേർഡ് പാർട്ടി വെബ്സൈറ്റുകളിൽ നിന്നുള്ള ആപ്പുകൾ ഡൗൺലോഡ് ചെയ്യുന്നത് ഒഴിവാക്കുക. ആപ്പുകൾ ഇൻസ്റ്റാൾ ചെയ്യുമ്പോൾ അവ ചോദിക്കുന്ന പെർമിഷനുകൾ അത്യാവശ്യമാണോ എന്ന് പരിശോധിക്കുക.

8. മൊബൈൽ ഫോണുകളിലെയും കമ്പ്യൂട്ടറുകളിലെയും മാൽവെയറുകളും വൈറസുകളും കണ്ടെത്തി നീക്കം ചെയ്യുന്നതിനായി ഭാരത സർക്കാരിന്റെ 'ബോട്ട്നെറ്റ് ക്ലീനിംഗ് ആൻഡ് മാൽവെയർ അനാലിസിസ് സെന്റർ' (Cyber Suraksha Kendra - CSK) നൽകുന്ന സൗജന്യ ആന്റി-വൈറസ്/ആന്റി-മാൽവെയർ ടൂളുകൾ https://www.csk.gov.in/security-tools.html എന്ന ഔദ്യോഗിക വെബ്സൈറ്റിൽ നിന്നും ഡൗൺലോഡ് ചെയ്ത് ഉപയോഗിക്കാവുന്നതാണ്.

9. ദീർഘനാളായി ഉപയോഗിക്കാത്ത ആപ്പുകൾ ഫോണിൽ നിന്ന് നീക്കം ചെയ്യുക (Uninstall). അവ നിങ്ങളുടെ ഡാറ്റ ചോർത്താൻ സാധ്യതയുണ്ട്.

10. ആവശ്യമില്ലാത്തപ്പോൾ ഫോണിലെ ലൊക്കേഷൻ സേവനങ്ങൾ ഓഫ് ചെയ്യുക. ഫോട്ടോകൾ പോസ്റ്റ് ചെയ്യുമ്പോൾ ലൊക്കേഷൻ ടാഗ് ചെയ്യുന്നത് ഒഴിവാക്കുക.

11. നിങ്ങളുടെ ഓരോ ക്ലിക്കും സുരക്ഷിതമാണെന്ന് ഉറപ്പുവരുത്തുക; കാരണം "ഇന്റർനെറ്റ് ഒന്നും മറക്കില്ല, ആരെയും മായ്ച്ചു കളയുകയുമില്ല!"

11. പാസ്വേഡ് സുരക്ഷ: പൊതുവായ മാർഗനിർദേശങ്ങൾ

ഡിജിറ്റൽ അക്കൗണ്ടുകളുടെയും ഉപകരണങ്ങളുടെയും സുരക്ഷ ഉറപ്പാക്കുന്നതിന് വിദ്യാർഥികളും അധ്യാപകരും രക്ഷിതാക്കളും വിദ്യാലയ അധികൃതരും ഒരുപോലെ താഴെ പറയുന്ന പാസ്വേഡ് മാനദണ്ഡങ്ങൾ പാലിക്കേണ്ടതാണ്:

1. ശക്തമായ പാസ്വേഡ് നിർമ്മാണം: അക്കങ്ങൾ, ചിഹ്നങ്ങൾ, വലിയ അക്ഷരങ്ങൾ (Uppercase), ചെറിയ അക്ഷരങ്ങൾ (Lowercase) എന്നിവ ചേർത്തുള്ള പാസ്വേഡുകൾ അല്ലെങ്കിൽ പാസ് ഫ്രേസുകൾ (Passphrases) മാത്രം ഉപയോഗിക്കുക.

2. ഏകീകൃത പാസ്വേഡ് ഒഴിവാക്കൽ: ഓരോ അക്കൗണ്ടിനും (ബാങ്കിംഗ്, സോഷ്യൽമീഡിയ, ഔദ്യോഗിക പോർട്ടലുകൾ) വ്യത്യസ്തമായ പാസ്വേഡുകൾ ഉപയോഗിക്കേണ്ടതാണ്; ഒരേ പാസ്വേഡ് എല്ലായിടത്തും ഉപയോഗിക്കുന്നത് ഒഴിവാക്കുക.

3. രഹസ്യാത്മകത: പാസ്വേഡുകൾ മറ്റാർക്കും ലഭ്യമാകുന്ന രീതിയിൽ ഡയറികളിലോ ഫോണിലെ നോട്ട്സിലോ കുറിച്ചു വെക്കാതിരിക്കുക. വ്യക്തിഗത പാസ്വേഡുകൾ സുഹൃത്തുക്കളുമായോ അപരിചിതരുമായോ യാതൊരു കാരണവശാലും പങ്കുവെക്കരുത്.

4. ഔദ്യോഗിക സുരക്ഷ: വിദ്യാലയങ്ങളിലെ വിവിധ സോഫ്റ്റ്വെയറുകൾ, ആപ്ലിക്കേഷനുകൾ എന്നിവയുടെ പാസ്വേഡുകൾ അതിന്റെ ചുമതലയുള്ളവർക്ക് മാത്രം ലഭ്യമാകുന്ന രീതിയിൽ ക്രമീകരിക്കണം. ഔദ്യോഗിക പാസ്വേഡുകൾ ബ്രൗസറുകളിൽ 'Autosave' ചെയ്യുന്നത് നിർബന്ധമായും ഒഴിവാക്കേണ്ടതാണ്.

5. ടു-ഫാക്ടർ ഓതന്റിക്കേഷൻ (2FA) : എല്ലാ സോഷ്യൽമീഡിയ, ബാങ്കിംഗ്, ഔദ്യോഗിക അക്കൗണ്ടുകളിലും അക്കൗണ്ട് സുരക്ഷയുടെ രണ്ടാം ഘട്ടമായ ടു-ഫാക്ടർ ഓതന്റിക്കേഷൻ (2FA/MFA) എനേബിൾ ചെയ്യുക.

6. വൈഫൈ (Wi-Fi) സുരക്ഷ : സ്കൂളിലെയും വീടുകളിലെയും വൈഫൈ നെറ്റ്വർക്കുകൾക്ക് ശക്തമായ പാസ്വേഡുകൾ നൽകുകയും ക്രമമായ ഇടവേളകളിൽ അവ മാറ്റുകയും ചെയ്യുക.

7. ലോഗൗട്ട് ശീലമാക്കുക : പൊതു കമ്പ്യൂട്ടറുകളോ ലാബുകളോ ഉപയോഗിച്ച ശേഷം ലോഗിൻ ചെയ്ത വെബ്സൈറ്റുകളിൽ നിന്നും ക്രമമായി ലോഗൗട്ട് ചെയ്യുക.

8. പാസ്വേഡ് പ്രൊട്ടക്ടഡ് : ഫോട്ടോകളും മറ്റ് രഹസ്യാത്മക ഫയലുകളും പാസ്വേഡ് ഉപയോഗിച്ച് സുരക്ഷിതമാക്കിയ ശേഷം (Password Protected) മാത്രം മറ്റുള്ളവരുമായി പങ്കുവെക്കുന്നതാണ് നല്ലത് . വിദ്യാലയങ്ങളിലും വീടുകളിലും വ്യക്തിഗത വിവരങ്ങൾ കൈകാര്യം ചെയ്യുമ്പോൾ ഡാറ്റാ സുരക്ഷിതത്വം ഉറപ്പാക്കാൻ ഇത് സഹായിക്കും.

12. പരാതി സമർപ്പിക്കലും പരിഹാര രീതിയും

സൈബർ സുരക്ഷിതത്വം ഓരോ വ്യക്തിയുടെയും അവകാശമാണ്. ഇത് ലംഘിക്കപ്പെടുന്ന സാഹചര്യം തിരിച്ചറിയാനുള്ള അടിസ്ഥാന അറിവ് കുട്ടികളും അധ്യാപകരും രക്ഷിതാക്കളും നേടിയിരിക്കണം. അതോടൊപ്പം ഇത്തരം കുറ്റകൃത്യങ്ങൾ ശ്രദ്ധയിൽ പെട്ടാൽ എങ്ങനെ കൈകാര്യം ചെയ്യണം എന്നതും അറിഞ്ഞിരിക്കേണ്ടതാണ്.

സൈബർ ആക്രമണമോ ചൂഷണമോ ഉണ്ടായാൽ കേവലം സ്കൂൾ തലത്തിൽ ഒതുക്കാതെ താഴെ പറയുന്ന നിയമവഴികൾ സ്വീകരിക്കണം:

1. സ്കൂൾ സൈബർ സേഫ്റ്റി കോർഡിനേറ്ററെയോ പ്രഥമാധ്യാപകരെയോ രക്ഷിതാക്കളെയോ ക്ലാസ് ടീച്ചറെയോ വിവരം അറിയിക്കുക. **(ഘട്ടം 1)**

2. നിയമ നടപടി: സാമ്പത്തിക തട്ടിപ്പുകൾക്കോ വ്യക്തിഹത്യകൾക്കോ ഇരയായാൽ ഉടൻ തന്നെ 1930 എന്ന നമ്പറിൽ വിളിക്കുകയോ www.cybercrime.gov.in എന്ന നാഷണൽ സൈബർ ക്രൈം റിപ്പോർട്ടിംഗ് പോർട്ടൽ വഴി പരാതി രജിസ്റ്റർ ചെയ്യുകയോ ചെയ്യുക. **(ഘട്ടം 2)**

3. പോലീസ് പരാതി: ഗുരുതരമായ കുറ്റകൃത്യങ്ങളിൽ (ഉദാഹരണത്തിന് മോർഫിംഗ്, ബ്ലാക്ക്മെയിലിംഗ്) അടുത്തുള്ള പോലീസ് സ്റ്റേഷനിലോ സൈബർ സെല്ലിലോ നേരിട്ട് പരാതി നൽകണം. **(ഘട്ടം 3)**

4. ഹെൽപ്പ് ലൈനുകൾ: കേരള പോലീസിന്റെ സൈബർ ഹെൽപ്പ് ലൈൻ 1090, കുട്ടികൾക്കായുള്ള ചൈൽഡ് ലൈൻ 1098 എന്നിവ പ്രയോജനപ്പെടുത്തുക.

13. ഡാറ്റാ സംരക്ഷണ നിയമവും കുട്ടികളും

ഡിജിറ്റൽ പേഴ്സണൽ ഡാറ്റാ പ്രൊട്ടക്ഷൻ ആക്ട് (DPDP Act) 2023-ൽ കേന്ദ്ര സർക്കാർ പാസാക്കിയിട്ടുണ്ടെങ്കിലും അതിന്റെ ചട്ടങ്ങൾ (Rules) പൂർണ്ണമായും വിജ്ഞാപനം ചെയ്യാത്തതിനാൽ ഇത് നിലവിൽ ഭാഗികമായി മാത്രമേ നടപ്പിലാക്കപ്പെട്ടിട്ടുള്ളൂ. എങ്കിലും, കുട്ടികളുടെയും (18 വയസ്സിൽ താഴെയുള്ളവർ) ശാരീരിക-മാനസിക വെല്ലുവിളികൾ നേരിടുന്നവരുടെയും ഡാറ്റ കൈകാര്യം ചെയ്യുന്നതിൽ അതീവ ജാഗ്രത വേണമെന്ന് ഈ നിയമം നിഷ്കർഷിക്കുന്നു.

നിയമത്തിലെ ശ്രദ്ധിക്കേണ്ട കാര്യങ്ങൾ

1. ഡാറ്റാ രക്ഷാധികാരി (Data Fiduciary): കുട്ടികളുടെ വിവരങ്ങൾ ശേഖരിക്കുന്ന സ്കൂളുകളോ ആപ്പുകളോ നിയമത്തിലെ 'ഡാറ്റാ ഫിഡുഷ്യറി' എന്ന നിർവചനത്തിനകത്ത് വരുന്നവരാണ്.

അതുകൊണ്ടുതന്നെ ഇന്റർനെറ്റ് പ്ലാറ്റ്ഫോമുകളെ പോലെ സ്കൂളിൽ ശേഖരിക്കുന്ന വിവരങ്ങളുടെ സുരക്ഷയ്ക്ക് ഉത്തരവാദികളാണ്.

2. പിഴ: ഈ നിയമത്തിലെ വ്യവസ്ഥകൾ ലംഘിക്കുന്ന സ്ഥാപനങ്ങൾക്ക് 200 കോടി രൂപ വരെ പിഴ ചുമത്താൻ വ്യവസ്ഥയുണ്ട്.

3. ഐ.ടി. ആക്ട് 2000: DPDP നിയമം പൂർണ്ണമായി നടപ്പിലാക്കുന്നത് വരെ ഐ.ടി. ആക്ട് 2000-ലെ (IT Act 2000) വകുപ്പുകൾ തുടരും. ഐ.ടി. ആക്ട് സെക്ഷൻ 43A റദ്ദാക്കിയെങ്കിലും സെക്ഷൻ 43 പ്രകാരമുള്ള സിവിൽ നടപടികൾ ഇപ്പോഴും നിലവിലുണ്ട്.

4. കുട്ടികളുടെ സൈബർ സുരക്ഷയും സ്വകാര്യതയുമായി ബന്ധപ്പെട്ട ഈ നിയമത്തിലെ പ്രധാന വ്യവസ്ഥകൾ അനുബന്ധം (അനുബന്ധം 2) ആയി നൽകുന്നു. ഇവ നിലവിൽ വരുന്ന മുറയ്ക്ക് അതിനായി പ്രത്യേക മാർഗനിർദേശങ്ങൾ പുറപ്പെടുവിക്കുന്നതാണ്.

5. ഐ.ടി. ചട്ട ഭേദഗതി (2026) നിർദേശങ്ങളിലും ഇതുമായി ബന്ധപ്പെട്ട പരാമർശമുണ്ട്. ഇതിൽ പ്രധാനപ്പെട്ടവ അനുബന്ധമായി (അനുബന്ധം 3) നൽകിയിട്ടുണ്ട്. ഇതിനു പുറമെ ഭാരതീയ ന്യായ സംഹിത (BNS), പോക്സോ നിയമം (POCSO Act) തുടങ്ങിയ നിയമങ്ങളിലും കുട്ടികളുടെ സൈബർസുരക്ഷാ ലംഘനങ്ങളെക്കുറിച്ച് കർശനമായ ശിക്ഷാ വ്യവസ്ഥകൾ നിഷ്കർഷിക്കുന്നുണ്ട്.

14. അറിയിക്കലും സൈബർ സേഫ്റ്റി ഓഡിറ്റിങ്ങും

പ്രോട്ടോക്കോളിൽ പറഞ്ഞിരിക്കുന്ന കാര്യങ്ങൾ എല്ലാ കുട്ടികളിലും അധ്യാപകരിലും രക്ഷിതാക്കളിലും കൃത്യമായി എത്തേണ്ടതുണ്ട്. ഇതിനായി എല്ലാ വിഭാഗങ്ങളെയും ഉൾക്കൊള്ളുന്ന വിധത്തിലുള്ള പരിശീലനങ്ങൾ സംഘടിപ്പിക്കണം. മാത്രമല്ല സ്കൂളിലെ ഇതുമായി ബന്ധപ്പെട്ട പ്രവർത്തനങ്ങൾ ഓഡിറ്റിംഗിന് വിധേയമാക്കുകയും വേണം.

സൈബർ സേഫ്റ്റി ഓഡിറ്റിംഗ്

ഇന്റർനെറ്റ് സൗകര്യം ഉപയോഗപ്പെടുത്തി കുട്ടികൾ വിവിധ തലത്തിൽ ചൂഷണം ചെയ്യപ്പെടുന്ന സംഭവങ്ങൾ ഗൗരവമർഹിക്കുന്ന വിഷയമാണ്. ആയതിനാൽ അത്തരം സന്ദർഭങ്ങൾ ഉണ്ടാകാതിരിക്കാൻ അധ്യാപകരും വിദ്യാർഥികളും രക്ഷിതാക്കളും പൊതുസമൂഹവും ജാഗ്രതയോടെ പ്രവർത്തിക്കേണ്ടതാണ്.

സ്കൂളിൽ സൈബർ സുരക്ഷാ ഓഡിറ്റിംഗ് നടത്തുന്നതിലൂടെ കൂടുതൽ ജാഗ്രതയോടെ സ്കൂളിന് പ്രവർത്തിക്കാനാകും. ഇതിനായി അധ്യാപകരും കുട്ടികളും രക്ഷിതാക്കളും ഉൾപ്പെടുന്ന ഒരു സൈബർ സേഫ്റ്റി ഓഡിറ്റിംഗ് ടീമിനെ നിയോഗിക്കാവുന്നതാണ്. ഓഡിറ്റിംഗിനായി ഉപയോഗിക്കാവുന്ന ചെക്ക്ലിസ്റ്റിന്റെ മാതൃക അനുബന്ധമായി നൽകിയിട്ടുണ്ട്. (അനുബന്ധം 4).

ഇതിനു പുറമെ, സ്കൂളിലെ ലാബിലും പൊതു ഇടങ്ങളിലും സൈബർ സേഫ്റ്റിയുമായി ബന്ധപ്പെട്ട പോസ്റ്ററുകൾ പതിക്കാവുന്നതാണ്. ഇതിന്റെ മാതൃകയും അനുബന്ധമായി നൽകിയിട്ടുണ്ട് (അനുബന്ധം 5, അനുബന്ധം 6). ഡിജിറ്റൽ സേഫ്റ്റിയെകുറിച്ചുള്ള അവബോധം നൽകുന്ന ക്ലാസുകളും സെമിനാറുകളും സംഘടിപ്പിക്കുമ്പോൾ സൈബർ സുരക്ഷാപ്രതിജ്ഞ (Cyber Safety Pledge) എടുക്കുന്നതിലൂടെ (അനുബന്ധം 7) ഇതുമായി ബന്ധപ്പെട്ട സന്ദേശം കൂടുതൽ ദൃഢമാകുന്നു.

അനുബന്ധം 1

സൈബർ കുറ്റകൃത്യങ്ങൾ, നിയമവകുപ്പുകൾ, പ്രതിരോധ മാർഗങ്ങൾ

കുട്ടികൾക്ക് സ്വയം മനസ്സിലാക്കാവുന്ന രീതിയിൽ വിശദീകരിച്ച ഏതാനും സൈബർ കുറ്റകൃത്യങ്ങളുടെ പട്ടിക താഴെ നൽകുന്നു. ഇതിൽ IT Act 2000, പുതിയ ഭാരതീയ ന്യായ സംഹിത (BNS 2023) എന്നിവയിലെ പ്രസക്തമായ വകുപ്പുകളും ഉൾപ്പെടുത്തിയിട്ടുണ്ട്.

ക്രമ നം	കുറ്റകൃത്യം (Crime)	വിശദീകരണം	നിയമവകുപ്പുകൾ (Sections)	മുൻകരുതലുകൾ
1	സ്വകാര്യതാ ലംഘനം (Violation of Privacy)	ഒരാളുടെ സമ്മതമില്ലാതെ സ്വകാര്യ ഭാഗങ്ങളുടെ ദൃശ്യങ്ങൾ പകർത്തുകയോ പ്രചരിപ്പിക്കുകയോ ചെയ്യുന്നത്.	IT Act Sec 66E.	ഉപയോഗിക്കാത്ത സമയത്ത് കാമറകൾ മറച്ചു വെക്കുക.
2	അശ്ലീലത (Obscenity)	മോശമായ ചിത്രങ്ങളോ വീഡിയോകളോ ഇന്റർനെറ്റിൽ പങ്കുവെക്കുന്നതും പ്രചരിപ്പിക്കുന്നതും ഇതിൽ വരുന്നു.	IT Act Sec 67, 67A	മാന്യമല്ലാത്ത സന്ദേശങ്ങളോ ചിത്രങ്ങളോ അയക്കാതിരിക്കുക
3	സൈബർ സ്റ്റാക്കിംഗ് (Cyber Stalking)	ഒരാളെ ഓൺലൈനിൽ നിരന്തരം നിരീക്ഷിക്കുകയും മെസേജുകൾ അയച്ച് ശല്യം ചെയ്യുകയും ഭീഷണിപ്പെടുത്തുകയും ചെയ്യുന്നത്.	IT Act Sec 66, BNS Sec 78	അപരിചിതരുടെ ഫ്രണ്ട് റിക്വസ്റ്റുകൾ സ്വീകരിക്കരുത്.
4	ഫിഷിംഗ് (Phishing)	ബാങ്കിൽ നിന്നാണെന്നോ ലോട്ടറി അടിച്ചെന്നോ വ്യാജേന വിശ്വസിപ്പിച്ച് നമ്മുടെ രഹസ്യവിവരങ്ങൾ തട്ടിയെടുക്കുന്ന രീതി.	IT Act Sec 66D	സമ്മാനങ്ങൾ വാഗ്ദാനം ചെയ്യുന്ന ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യരുത്.
5	ഡീപ്ഫെയ്ക് (Deepfake)	ആർട്ടിഫിഷ്യൽ ഇന്റലിജൻസ് ഉപയോഗിച്ച് ഒരാളുടെ മുഖവും ശബ്ദവും മാറ്റി വ്യാജ വീഡിയോകളോ ചിത്രങ്ങളോ നിർമ്മിക്കുന്നത്.	IT Act Sec 66D, 66E	സംശയാസ്പദമായ വീഡിയോകൾ ഷെയർ ചെയ്യരുത്.
6	ഐഡന്റിറ്റി മോഷണം (Identity Theft)	മറ്റൊരാളുടെ പാസ്‌വേഡോ മറ്റ് രേഖകളോ ഉപയോഗിച്ച് അവരുടെ പേരിൽ വഞ്ചന നടത്തുന്നത് ഇതിൽ വരുന്നു.	IT Act Sec 66C	ശക്തമായ പാസ്‌വേഡുകൾ ഉപയോഗിക്കുക.
7	ആൾമാറാട്ടം (Impersonation)	മറ്റൊരാളാണെന്ന് തെറ്റായി ധരിപ്പിച്ച് (ഉദാഹരണത്തിന് വ്യാജ അക്കൗണ്ട് വഴി) ലാഭമുണ്ടാക്കാനോ ഉപദ്രവിക്കാനോ ശ്രമിക്കുന്നത്.	IT Act Sec 66D	പ്രൊഫൈലുകളുടെ ആധികാരികത പരിശോധിക്കുക.
8	ഓൺലൈൻ ഗ്രൂമിംഗ് (Grooming)	കുട്ടികളെ മോശമായ കാര്യങ്ങൾക്കായി കെണിയിൽ പെടുത്താൻ മുതിർന്നവർ സൗഹൃദം അഭിനയിച്ച് അടുക്കുന്ന രീതിയാണിത്.	POCSO Act Sec 11(iv), 11(vi), 13, 15	ഓൺലൈൻ സുഹൃത്തുക്കളെ ഒറ്റയ്ക്ക് നേരിട്ട് കാണരുത്.
9	ഡാറ്റാ ബ്രീച്ച് (Data Breach)	നമ്മുടെ അനുവാദമില്ലാതെ നമ്മുടെ രഹസ്യ വിവരങ്ങൾ (ഫോട്ടോ, ഫോൺ നമ്പർ തുടങ്ങിയവ) മറ്റൊരാൾ കൈക്കലാക്കുന്നത് ഇതിൽ വരുന്നു.	DPDP Act 2023 IT Act Sec 66	സുരക്ഷിതമായ ആപ്പുകൾ മാത്രം ഉപയോഗിക്കുക.
10	കാമറ ഹാക്കിംഗ് (Camera Hacking)	നാമറിയാതെ നമ്മുടെ ഫോണിലെ ലാപ്ടോപ്പിലെ കാമറ പ്രവർത്തിപ്പിച്ച് രഹസ്യങ്ങൾ ചോർത്തുന്ന രീതിയാണിത്.	IT Act Sec 66	ആവശ്യമില്ലാത്ത ആപ്പുകൾ ഇൻസ്റ്റാൾ ചെയ്യരുത്.

11	സെക്സ്റ്റിംഗ് (Sexting)	സ്വകാര്യ ചിത്രങ്ങൾ സന്ദേശമായി അയക്കുന്നത് കുറ്റകരമാണ്. കുട്ടികൾക്കിടയിൽ ഇത് നടന്നാലും പോക്സോ നിയമപ്രകാരം ശിക്ഷ ലഭിക്കാം.	IT Act Sec 67, POCSO Act	സ്വകാര്യ ചിത്രങ്ങൾ ഓൺലൈനിൽ പങ്കുവെക്കരുത്.
12	സൈബർ ബുള്ളിയിങ് (Cyber Bullying)	സോഷ്യൽ മീഡിയയിലൂടെയോ ഗെയിമിംഗ് വഴിയോ ഒരാളെ കളിയാക്കുന്നതും അപമാനിക്കുന്നതും ഇതിൽ വരുന്നു.		ഓൺലൈനിൽ എല്ലാവരോടും മാന്യമായി പെരുമാറുക.
13	വ്യാജ വാർത്ത പ്രചരിപ്പിക്കൽ (Fake News)	തെറ്റായ വാർത്തകൾ പ്രചരിപ്പിക്കുന്നത് കുറ്റകരമാണ്. ഇത് സമൂഹത്തിൽ വലിയ പ്രശ്നങ്ങൾക്ക് കാരണമാകും.	IT Rules 2021/2026	ഉറവിടം അറിയാത്ത വിവരങ്ങൾ ഷെയർ ചെയ്യരുത്.
14	ഹാക്കിംഗ് (Hacking)	മറ്റൊരാളുടെ അനുവാദമില്ലാതെ അവരുടെ കമ്പ്യൂട്ടറിലോ ഇന്റർനെറ്റ് അക്കൗണ്ടിലോ നുഴഞ്ഞുകയറുന്നത് ഇതിൽ വരുന്നു.	IT Act Sec 66	പാസ്വേഡുകൾ ആരുമായും പങ്കുവെക്കരുത്.
15	സ്പൂഫിംഗ് (Spoofing)	യഥാർഥ വിലാസം മറച്ചുവെച്ച് മറ്റൊരാളാണെന്ന ഭാവത്തിൽ മെസേജുകളോ ഇമെയിലോ അയക്കുന്ന തട്ടിപ്പാണിത്.	IT Act Sec 66D	സംശയാസ്പദമായ ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യരുത്.
16	സെക്സ്റ്റോർഷൻ (Sextortion)	സ്വകാര്യ ദൃശ്യങ്ങൾ കൈക്കലാക്കി അത് പുറത്തുവിടുമെന്ന് ഭീഷണിപ്പെടുത്തി പണമോ മറ്റ് കാര്യങ്ങളോ ആവശ്യപ്പെടുന്നത് അതീവ ഗുരുതരമായ കുറ്റമാണ്.	IT Act Sec 66, 67, BNS Sec 308	ഭീഷണികൾക്ക് വഴങ്ങരുത്; ഉടൻ അധ്യാപകരെയോ പോലീസിനെയോ അറിയിക്കുക.
17	CSAM (Child Sexual Abuse Material)	കുട്ടികളെ ലൈംഗികമായി ചൂഷണം ചെയ്യുന്നതോ ദുരുപയോഗം ചെയ്യുന്നതോ ആയ ദൃശ്യങ്ങൾ, വീഡിയോകൾ, ശബ്ദരേഖകൾ തുടങ്ങിയവ	IT Act Sec 67B, 67B(b) POCSO Sec 15, 15(3)	സ്വകാര്യ ചിത്രങ്ങൾ ഓൺലൈനിൽ പങ്കുവെക്കരുത്. ഇത്തരം മെറ്റീരിയലുകൾ കണ്ടാൽ ബന്ധപ്പെട്ടവരെ അറിയിക്കുക.
18	ഡിജിറ്റൽ അറസ്റ്റ് (Digital Arrest)	പോലീസ്, നർക്കോട്ടിക്സ് ബ്യൂറോ (NCB), സി.ബി.ഐ (CBI) തുടങ്ങിയ അന്വേഷണ ഏജൻസികളിലെ ഉദ്യോഗസ്ഥരാണെന്ന വ്യാജേന വീഡിയോ കോളിലൂടെയും മറ്റും ഭീഷണിപ്പെടുത്തി തടങ്കലിൽ വെക്കുന്ന രീതിയിലുള്ള സൈബർ തട്ടിപ്പ്	BNS Sec 61, 127, 204, 308, 319 (പുതിയ തരം ക്രൈമായതിനാൽ ഇതിനെ കൈകാര്യം ചെയ്യുന്നതിന് പ്രത്യേകമായി വകുപ്പുകൾ നിലവിലില്ല)	ഇന്ത്യൻ നിയമ വ്യവസ്ഥയിൽ 'ഡിജിറ്റൽ അറസ്റ്റ്' എന്നൊരു നടപടി നിലവിലില്ല. അതിനാൽ ഭയപ്പെടാതിരിക്കുക.
19	ട്രോളിംഗ് (Trolling)	മറ്റൊരാളെ മാനസികമായി തളർത്തുന്ന രീതിയിൽ അപകീർത്തികരമായ വീഡിയോകളോ സന്ദേശങ്ങളോ ഉണ്ടാക്കി പ്രചരിപ്പിക്കുന്നത് കുറ്റകരമാണ്.	IT Act Sec 66	മറ്റൊരാളെ വേദനിപ്പിക്കുന്ന തരത്തിലുള്ള ട്രോളുകൾ നിർമ്മിക്കരുത്.
20	എ.ഐ. ഗ്രൂമിംഗ് (AI Grooming)	ഓൺലൈൻ ഗ്രൂമിംഗിൽ ഒരു വ്യക്തി കുട്ടിയോട് നേരിട്ട് സംസാരിക്കുമ്പോൾ, ഇവിടെ എ.ഐ. ചാറ്റ്ബോട്ടുകളോ (Chatbots) ഡീപ്ഫേക്ക് (Deepfake) സാങ്കേതികവിദ്യയോ ആണ് വഞ്ചനയ്ക്കായി ഉപയോഗിക്കുന്നത്.	POCSO Act Sec 13-15	പരിചയമില്ലാത്തവരുമായി ഓൺലൈനിൽ ആശയവിനിമയം നടത്താതിരിക്കുക.

അനുബന്ധം 2

ഡിജിറ്റൽ പേഴ്സണൽ ഡാറ്റാ പ്രൊട്ടക്ഷൻ ആക്ടിൽ (DPDP Act) പരാമർശിച്ചിട്ടുള്ള കുട്ടികളുമായി ബന്ധപ്പെട്ട കുറ്റകൃത്യങ്ങളുടെ വിശദാംശങ്ങൾ താഴെ പട്ടികയിൽ നൽകിയിരിക്കുന്നു.

ക്രമനം	കുറ്റം (Offence)	വിശദീകരണം	വകുപ്പ് (Section)	മുൻകരുതലുകൾ	പരിഹാരം
1	അനുമതിയില്ലാത്ത ഡാറ്റാ ശേഖരണം	രക്ഷിതാക്കളുടെ സമ്മതമില്ലാതെ കുട്ടികളുടെ വ്യക്തിഗത വിവരങ്ങൾ ശേഖരിക്കുന്നത് കുറ്റകരമാണ്.	Sec 9(1)	കുട്ടികൾ ഉപയോഗിക്കുന്ന ആപ്പുകളിൽ രക്ഷിതാക്കളുടെ ഇ-മെയിൽ/ഫോൺ നമ്പർ വഴി സമ്മതം (Parental Consent) നൽകുക.	വിവരങ്ങൾ തെറ്റായി ശേഖരിച്ചാൽ അത് തിരുത്താനോ നീക്കം ചെയ്യാനോ (Right to Erasure) ആവശ്യപ്പെടാം.
2	കുട്ടികളെ നിരീക്ഷിക്കൽ (Tracking/ Monitoring)	കുട്ടികളുടെ ഓൺലൈൻ പെരുമാറ്റം നിരീക്ഷിക്കുന്നതോ അവരെ ട്രാക്ക് ചെയ്യുന്നതോ ആയ സാങ്കേതികവിദ്യകൾ ഉപയോഗിക്കാൻ പാടില്ല.	Sec 9(3)	ബ്രൗസറുകളിൽ 'Do Not Track' ഓപ്ഷൻ ഓൺ ചെയ്യുക. ലൊക്കേഷൻ പെർമിഷനുകൾ ഒഴിവാക്കുക.	ഡാറ്റാ പ്രൊട്ടക്ഷൻ ബോർഡിന് (DPB) പരാതി നൽകുക.
3	ലക്ഷ്യം വെച്ചുള്ള പരസ്യങ്ങൾ (Targeted Advertising)	കുട്ടികളെ ലക്ഷ്യമിട്ടുള്ള പരസ്യങ്ങൾ പ്രദർശിപ്പിക്കുന്നതിനായി അവരുടെ വിവരങ്ങൾ ഉപയോഗിക്കുന്നത് നിയമം വിലക്കുന്നു.	Sec 9(3)	ആപ്പുകളുടെ പ്രൈവസി സെറ്റിംഗുകളിൽ 'Ad Personalization' ഓഫ് ചെയ്യുക.	പ്ലാറ്റ്ഫോമിലെ റിപ്പോർട്ടിംഗ് സംവിധാനം ഉപയോഗിക്കുക.
4	ഹാനികരമായ ഡാറ്റാ പ്രോസസ്സിംഗ്	കുട്ടികളുടെ ശാരീരികമോ മാനസികമോ ആയ ആരോഗ്യത്തെ ബാധിക്കുന്ന തരത്തിൽ വിവരങ്ങൾ ഉപയോഗിക്കുന്നത് ശിക്ഷാർഹമാണ്	Sec 9(2)	അപരിചിതമായ വെബ്സൈറ്റുകളിൽ കുട്ടികളുടെ ചിത്രം, സ്കൂൾ വിവരങ്ങൾ എന്നിവ	നാഷണൽ സൈബർ ക്രൈം പോർട്ടൽ (1930) വഴിയോ പോലീസിലോ പരാതിപ്പെടുക

അനുബന്ധം 3

ഐ.ടി. ചട്ട ഭേദഗതി 2026
പ്രധാന നിർദേശങ്ങൾ

1. എ.ഐ. (AI) ഉള്ളടക്കം തിരിച്ചറിയുക: എ.ഐ. സാങ്കേതികവിദ്യ ഉപയോഗിച്ച് നിർമ്മിച്ചതോ മാറ്റം വരുത്തിയതോ ആയ ചിത്രങ്ങൾ, ഓഡിയോ, വീഡിയോ എന്നിവയെ 'സിന്തറ്റിക്കലി ജനറേറ്റഡ് ഇൻഫർമേഷൻ' (SGI) എന്ന് വിളിക്കുന്നു. ഇവ യഥാർഥമാണെന്ന് തോന്നിപ്പിക്കുമെങ്കിലും വ്യാജമായിരിക്കാം. ഇത്തരം ഉള്ളടക്കങ്ങളിൽ 'AI നിർമ്മിതം' എന്ന ലേബൽ ഉണ്ടോ എന്ന് നിർബന്ധമായും പരിശോധിക്കേണ്ടതാണ്.

2. വ്യാജ ദൃശ്യങ്ങൾക്കെതിരെയുള്ള ജാഗ്രത: ഒരാളുടെ രൂപമോ ശബ്ദമോ എ.ഐ. ഉപയോഗിച്ച് മാറ്റി വ്യാജമായി നിർമ്മിക്കുന്നത് നിയമവിരുദ്ധമാണ്. ഇത്തരം ആധികാരികതയില്ലാത്ത വീഡിയോകളോ വോയ്സ് ക്ലിപ്പുകളോ ആർക്കും ഫോർവേഡ് ചെയ്യരുത്.

3. അടിയന്തര റിപ്പോർട്ടിംഗും നടപടിയും: കുട്ടികൾക്കെതിരെയുള്ള അതിക്രമങ്ങൾ, അനുവാദമില്ലാതെയുള്ള സ്വകാര്യ ദൃശ്യങ്ങൾ, ഡീപ്ഫേക്കുകൾ എന്നിവ ശ്രദ്ധയിൽപ്പെട്ടാൽ ഉടൻ റിപ്പോർട്ട് ചെയ്യുക. പുതിയ നിയമപ്രകാരം ഇത്തരം പരാതികളിൽ സോഷ്യൽ മീഡിയ പ്ലാറ്റ്ഫോമുകൾ രണ്ട് മണിക്കൂറിനുള്ളിൽ നടപടി സ്വീകരിക്കേണ്ടതുണ്ട്.

അനുബന്ധം 4

സൈബർ സേഫ്റ്റി ഓഡിറ്റ് - ചെക്ക് ലിസ്റ്റ്

1	സ്കൂളിലെ കമ്പ്യൂട്ടറുകളിൽ ക്ലാസുകൾക്കും/അധ്യാപകർക്കും പ്രത്യേകം ലോഗിനുകൾ നിർമ്മിച്ചിട്ടുണ്ട്.	
2	എല്ലാ കമ്പ്യൂട്ടറുകളും ലാപ്ടോപ്പുകളും പാസ്വേഡ് ഉപയോഗിച്ച് സുരക്ഷിതമാക്കിയിട്ടുണ്ട്.	
3	സ്കൂളിലെ Wi-Fi ശക്തമായ പാസ്വേഡ് ഉപയോഗിച്ച് സുരക്ഷിതമാക്കിയിട്ടുണ്ട്. കൂടാതെ, സുരക്ഷ ഉറപ്പാക്കുന്നതിനായി ഈ പാസ്വേഡ് ക്രമമായ ഇടവേളകളിൽ മാറ്റുകയും ചെയ്യുന്നുണ്ട്.	
4	സ്കൂൾ ഇ-മെയിൽ സർക്കാർ അനുവദിച്ച സംവിധാനത്തിലാണ് പ്രവർത്തിക്കുന്നത്. ശക്തമായ പാസ്വേഡ് ഉപയോഗിച്ച് ഇ-മെയിൽ സംരക്ഷിക്കപ്പെട്ടിട്ടുണ്ട്.	
5	സ്കൂൾ ഇ-മെയിൽ ഉപയോഗിക്കുന്നത് പ്രധാന അധ്യാപകൻ / ചുമതലപ്പെടുത്തിയ ആൾ മാത്രമാണ് .	
6	സ്കൂൾ ഉപയോഗിക്കുന്ന വിവിധ ഇ-ഗവേണൻസ് സംവിധാനങ്ങൾ അനുവദിക്കപ്പെട്ടവർ മാത്രമാണ് ഉപയോഗിക്കുന്നത് എന്ന് ഉറപ്പാക്കിയിട്ടുണ്ട്.	
7	കുട്ടികളുടെ വ്യക്തിഗത വിവരങ്ങൾ സർക്കാർ നിർദേശിക്കുന്ന വെബ്സൈറ്റുകളിൽ മാത്രമാണ് ശേഖരിക്കപ്പെടുന്നത് എന്ന് ഉറപ്പാക്കിയിട്ടുണ്ട്.	
8	കുട്ടികൾ ഉൾപ്പെടുന്ന ഉള്ളടക്കം സമൂഹമാധ്യമങ്ങളിൽ പങ്കു വയ്ക്കുമ്പോൾ സ്വകാര്യതാ ലംഘനം നടന്നിട്ടില്ല എന്ന് ഉറപ്പുവരുത്തിയിട്ടുണ്ട്.	
9	സ്കൂൾ ശേഖരിച്ച ഡിജിറ്റൽ വിവരങ്ങൾ ക്രമമായ ഇടവേളകളിൽ back-up ചെയ്തു വയ്ക്കാറുണ്ട്.	
10	കുട്ടികൾ ഉപയോഗിക്കുന്ന കമ്പ്യൂട്ടറുകൾ / ലാപ്ടോപ്പുകൾ എന്നിവയുടെ സ്ക്രീൻ എല്ലാവർക്കും കാണാനാവുന്ന വിധത്തിലാണ് സജ്ജീകരിച്ചിരിക്കുന്നത്.	
11	സൈബർ സുരക്ഷ സംബന്ധിച്ച് അധ്യാപകർ, വിദ്യാർഥികൾ, രക്ഷിതാക്കൾ എന്നിവർക്ക് സർക്കാർ നിഷ്കർഷിക്കുന്ന ഇടവേളകളിൽ പരിശീലനം നൽകിയിട്ടുണ്ട്.	
12	ഏതെങ്കിലും തരത്തിലുള്ള സൈബർ കുറ്റകൃത്യത്തിന് വിധേയനായാൽ എന്താണ് ചെയ്യേണ്ടത് എന്നത് സംബന്ധിച്ച നിർദേശങ്ങൾ അടങ്ങിയ ബോർഡ് പൊതു ഇടങ്ങളിൽ പ്രദർശിപ്പിച്ചിട്ടുണ്ട്.	

[സ്കൂളിന്റെ സാഹചര്യത്തിനനുസരിച്ച് കൂടുതൽ ഇനങ്ങൾ കൂട്ടിച്ചേർക്കാം.]

അനുബന്ധം 5

സുരക്ഷിതമായ ഇന്റർനെറ്റ് ഉപയോഗവുമായി ബന്ധപ്പെട്ട്
കമ്പ്യൂട്ടർ ലാബിൽ പ്രദർശിപ്പിക്കേണ്ട നോട്ടീസ്

സുരക്ഷിതമായ ഇന്റർനെറ്റ് ഉപയോഗം

✔ ചെയ്യേണ്ടത്

- *ടീച്ചർ നിർദേശിച്ച വിദ്യാഭ്യാസ സൈറ്റുകൾ മാത്രം ഉപയോഗിക്കുക.*
- *ശക്തമായ പാസ്‌വേഡ് ഉപയോഗിക്കുക.*
- *ലോഗിൻ ചെയ്ത സൈറ്റുകൾ ഉപയോഗത്തിന് ശേഷം ലോഗൗട്ട് ചെയ്യുക*
- *"https://" ഉള്ള സുരക്ഷിത വെബ്സൈറ്റുകൾ മാത്രം തുറക്കുക.*
- *സംശയാസ്പദമായ ഉള്ളടക്കം കണ്ടാൽ ഉടൻ ടീച്ചറെ അറിയിക്കുക.*
- *ഓൺലൈനിൽ എല്ലാവരോടും മാന്യമായി പെരുമാറുക.*
- *ഡൗൺലോഡ് ചെയ്യുമ്പോൾ പകർപ്പവകാശ നിയമം പാലിക്കുക.*
- *ഡിജിറ്റൽ ഫൂട്ട്പ്രിന്റ് ഓർക്കുക: ഓൺലൈനിൽ പോസ്റ്റ് ചെയ്യുന്ന ഓരോ കാര്യവും നമ്മുടെ സ്ഥിരമായ ഡിജിറ്റൽ രേഖയായി മാറാം. പോസ്റ്റ് ചെയ്യുന്നതിന് മുമ്പ് രണ്ടുതവണ ചിന്തിക്കുക.*

✘ ചെയ്യാൻ പാടില്ലാത്തത്

- *വ്യക്തിഗത വിവരങ്ങൾ (വിലാസം, ഫോൺ നമ്പർ, പാസ്‌വേഡ്, വീടിന്റെ ലൊക്കേഷൻ) പങ്കിടരുത്.*
- *അനുമതിയില്ലാതെ സോഫ്റ്റ്വെയർ/ആപ്പുകൾ ഡൗൺലോഡ് ചെയ്യരുത്.*
- *അപമാനകരമായ സന്ദേശങ്ങൾ അയക്കരുത്.*
- *സ്കൂൾ സമയത്ത് സോഷ്യൽമീഡിയ ഉപയോഗിക്കരുത്.*

സൈബർ കുറ്റകൃത്യങ്ങൾ അറിയിക്കേണ്ട നമ്പർ : 1930

അനുബന്ധം 6

സൈബർ സുരക്ഷയുമായി ബന്ധപ്പെട്ട് സ്കൂൾ നോട്ടീസ് ബോർഡിൽ പ്രദർശിപ്പിക്കേണ്ട നോട്ടീസ്

സൈബർ സുരക്ഷാ വിദ്യാലയം

- ഈ സ്കൂളിലെ വിദ്യാർഥികൾ അധ്യാപകരുടെ മേൽനോട്ടത്തിൽ മാത്രമേ ഇന്റർനെറ്റ് ഉപയോഗിക്കുന്നുള്ളൂ.
- ഈ സ്കൂളിലെ വിദ്യാർഥികൾക്ക് സുരക്ഷിതമായ ഇന്റർനെറ്റ് വിനിയോഗവുമായി ബന്ധപ്പെട്ടുള്ള നിർദേശങ്ങൾ സ്ഥിരമായി നൽകുന്നു.
- ഈ സ്കൂളിലെ വിദ്യാർഥികളുടെ വിവരങ്ങൾ സർക്കാർ നിർദേശിച്ച വെബ്സൈറ്റുകളുമായി മാത്രമേ പങ്കിടുന്നുള്ളൂ.
- പകർപ്പവകാശ നിയമമനുസരിച്ച് സ്വതന്ത്രമായി ഉപയോഗിക്കാൻ കഴിയുന്ന ഉള്ളടക്കങ്ങൾ മാത്രമേ ഇന്റർനെറ്റിൽ നിന്ന് ഡൗൺലോഡ് ചെയ്യുന്നുള്ളൂ.
- ഇവിടുത്തെ അധ്യാപകർക്കും വിദ്യാർഥികൾക്കും രക്ഷിതാക്കൾക്കും സൈബർ സുരക്ഷാ പരിശീലനങ്ങൾ സ്ഥിരമായി സംഘടിപ്പിക്കുന്നു.
- സൈബർ കുറ്റകൃത്യങ്ങൾ ശ്രദ്ധയിൽപെടുമ്പോൾ നിയമപരമായ നടപടികൾക്കായി ബന്ധപ്പെട്ട അധികാരികളെ ഞങ്ങൾ അറിയിക്കുന്നു.
- ഈ സ്കൂളിലെ കമ്പ്യൂട്ടറുകളിൽ സ്വതന്ത്ര സോഫ്റ്റ്വെയർ മാത്രമേ ഉപയോഗിക്കുന്നുള്ളൂ.

സൈബർ കുറ്റകൃത്യങ്ങൾ അറിയിക്കേണ്ട നമ്പർ : 1930

അനുബന്ധം 7

സൈബർ സുരക്ഷാ പ്രതിജ്ഞ

"ഡിജിറ്റൽ ലോകത്തെ ഉത്തരവാദിത്തമുള്ള പൗരരായി വളരുമെന്ന് ഞാൻ പ്രതിജ്ഞ ചെയ്യുന്നു.

എന്റെയും കുടുംബത്തിന്റെയും സ്വകാര്യവിവരങ്ങളും പാസ്‌വേഡുകളും മറ്റാരും ദുരുപയോഗം ചെയ്യാത്ത രീതിയിൽ ഞാൻ രഹസ്യമായി സൂക്ഷിക്കും. ഇന്റർനെറ്റിൽ പരിചയപ്പെടുന്ന അപരിചിതരുമായി വ്യക്തിബന്ധങ്ങൾ സ്ഥാപിക്കില്ലെന്നും സുരക്ഷിതമല്ലാത്ത ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യില്ലെന്നും ഞാൻ ഉറപ്പുനൽകുന്നു.

സഹപാഠികളെയോ മറ്റുള്ളവരെയോ ഓൺലൈൻ പ്ലാറ്റ്ഫോമുകളിൽ അപമാനിക്കുകയോ പരിഹസിക്കുകയോ ചെയ്യില്ല. സൈബർ ലോകത്തെ ചതിക്കുഴികളോ ബുദ്ധിമുട്ടുകളോ ശ്രദ്ധയിൽപ്പെട്ടാൽ ഒളിച്ചുവെക്കാതെ എന്റെ അധ്യാപകരെയോ രക്ഷിതാക്കളെയോ ഞാൻ അറിയിക്കും.

പഠനത്തിനും വിനോദത്തിനുമായി ഡിജിറ്റൽ ഉപകരണങ്ങൾ ഉപയോഗിക്കുമ്പോൾ ക്യത്യമായ സമയക്രമം പാലിക്കുമെന്നും, സാങ്കേതികവിദ്യയെ എന്റെയും സമൂഹത്തിന്റെയും നന്മയ്ക്കായി മാത്രം ഉപയോഗിക്കുമെന്നും ഇതിനാൽ ഞാൻ പ്രതിജ്ഞ ചെയ്യുന്നു.

സ്കൂൾ കുട്ടികൾക്കുവേണ്ടിയുള്ള

സൈബർ സേഫ്റ്റി പ്രോട്ടോക്കോൾ - 2026

പുറപ്പെടുവിക്കുന്നത് :

കേരള ഇൻഫ്രാസ്ട്രക്ചർ ആന്റ് ടെക്നോളജി ഫോർ എഡ്യൂക്കേഷൻ (കൈറ്റ്)

പൂജപ്പുര, തിരുവനന്തപുരം - 695012, www.kite.kerala.gov.in

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

സ്കൂൾ കുട്ടികൾക്കുവേണ്ടിയുള്ള

സൈബർ സേഫ്റ്റി പ്രോട്ടോക്കോൾ 2026

പൊതുവിദ്യാഭ്യാസവകുപ്പ്
കേരള സർക്കാർ

KERALA INFRASTRUCTURE AND TECHNOLOGY FOR EDUCATION

കേരള ഇൻഫ്രാസ്ട്രക്ചർ & ടെക്നോളജി
ഫോർ എഡ്യൂക്കേഷൻ (കൈറ്റ്)
പൂജപ്പുര, തിരുവനന്തപുരം - 695012
www.kite.kerala.gov.in, contact@kite.kerala.gov.in
Phone : 0471 2529800