Government of Kerala

KERALA INFRASTRUCTURE AND TECHNOLOGY FOR EDUCATION

No. KITE/2019/1605 (2)

തീയതി : 23.02.2019

സ്കൂൾ കുട്ടികൾക്കുവേണ്ടിയുള്ള സൈബർ സേഫ്റ്റി പ്രോട്ടോകോൾ

വിഷയം:- കൈറ്റ് – പതിമൂന്നാം കേരള നിയമസഭ – സ്ത്രീകളുടേയും കുട്ടികളുടേയും വികലാംഗരുടേയും ക്ഷേമം സംബന്ധിച്ച സമിതി (2011-14) – സ്കൂൾ കുട്ടികൾക്കുവേണ്ടി കേരള സ്റ്റേറ്റ് സൈബർ സേഫ്റ്റി പ്രോട്ടോകോൾ വികസിപ്പിച്ചെടുത്ത് അവ നടപ്പിലാക്കേണ്ടതാണെന്ന നിർദ്ദേശം – പ്രാവർത്തികമാക്കുന്നത് സംബന്ധിച്ച നിർദേശങ്ങൾ പുറപ്പെടുവിക്കുന്നു.

സൂചന:-

1. പതിമൂന്നാം കേരള നിയമസഭ സ്ത്രീകളുടേയും കുട്ടികളുടേയും വികലാംഗരുടേയും ക്ഷേമം സംബന്ധിച്ച സമിതിയുടെ (2011-14) ആറാമത് റിപ്പോർട്ടിലെ ഖണ്ഡിക 36 ലെ ശുപാർശ.
2. ഇലക്ട്രോണിക്സ് & വിവര സാങ്കേതിക വകുപ്പ് സെക്രട്ടറിയുടെ 18.05.18 ലെ ഐ.ടി.-സി2/259/16/വി.സ.വ നമ്പർ കത്ത്.
3. പൊതുവിദ്യാഭ്യാസ സെക്രട്ടറിയുടെ 27.06.2018 ലെ ഡി3/167/2018/ പൊ.വി.വ. നമ്പർ കത്ത്.

പതിമൂന്നാം കേരള നിയമസഭയുടെ സ്ത്രീകളുടേയും കുട്ടികളുടേയും വികലാംഗരുടേയും ക്ഷേമം സംബന്ധിച്ച സമിതിയുടെ (2011-14) ആറാമത് റിപ്പോർട്ടിലെ ഖണ്ഡിക 36 ൽ ഇന്റർനെറ്റ് സൗകര്യം പ്രയോജനപ്പെടുത്തി സോഷ്യൽ മീഡിയകളിലൂടെ കുട്ടികൾ വിവിധതരത്തിൽ ചൂഷണം ചെയ്യപ്പെടുന്ന സംഭവങ്ങൾ വർദ്ധിച്ചുവരുന്നത് ഗൗരവമർഹിക്കുന്ന ഒരു വിഷയമാണെന്നും ഇത് സംബന്ധിച്ച് മുന്നറിയിപ്പു നൽകിയുള്ള ബോധവൽക്കരണം ഇന്നത്തെ സൈബർ യുഗത്തിൽ അതിപ്രാധാന്യം അർഹിക്കുന്നു എന്നും ശുപാർശ ചെയ്തിട്ടുണ്ട്. സമിതിയുടെ ശുപാർശയുടെ അടിസ്ഥാനത്തിൽ കേരള ഇൻഫ്രാസ്ട്രക്ച്ചർ ആന്റ് ടെക്നോളജി ഫോർ എഡ്യൂക്കേഷൻ – കൈറ്റ് (മുൻ ഐ.ടി.@സ്കൂൾ പ്രോജക്ട്) സ്കൂൾ കുട്ടികൾക്കുവേണ്ടി കേരള സ്റ്റേറ്റ് സൈബർ സേഫ്റ്റി പ്രോട്ടോകോൾ വികസിപ്പിച്ചെടുത്ത് അവ നടപ്പിലാക്കേണ്ടതാണെന്ന് കേരള സ്റ്റേറ്റ് ഇൻഫർമേഷൻ ടെക്നോളജി മിഷൻ ഡയറക്ടർ നിർദ്ദേശം നൽകിയിട്ടുണ്ട്. ആയതിന്റെ അടിസ്ഥാനത്തിൽ സ്കൂൾ കുട്ടികൾക്കവേണ്ടി കേരള സ്റ്റേറ്റ് സൈബർ സേഫ്റ്റി പ്രോട്ടോക്കോൾ ഇതോടൊപ്പം പ്രസിദ്ധീകരിക്കുന്നു.

കെ. അൻവർ സാദത്ത്
വൈസ് ചെയർമാൻ & എക്സിക്യൂട്ടീവ് ഡയറക്ടർ

KERALA INFRASTRUCTURE AND
TECHNOLOGY FOR EDUCATION

സ്കൂൾ കുട്ടികൾക്കുള്ള സൈബർ സേഫ്റ്റി പ്രോട്ടോക്കോൾ

1. ആമുഖം	03
2. സൈബർ സേഫ്റ്റി ക്ലിനിക്കുകൾ	03
3. ഓഫീസ് മേധാവി ഉറപ്പുവരുത്തേണ്ട കാര്യങ്ങൾ	04
4. അധ്യാപകർ ഉറപ്പുവരുത്തേണ്ടത്	05
5. വിദ്യാർഥികൾ പാലിക്കേണ്ട കാര്യങ്ങൾ	05
6. രക്ഷിതാക്കൾ ശ്രദ്ധിക്കേണ്ട കാര്യങ്ങൾ	07
7. പൊതുനിർദേശങ്ങൾ	07

1. ആമുഖം

സംസ്ഥാനത്തെ സ്കൂളുകളിൽ ഐ.ടി, ഐ.സി.ടി. പഠനം ആരംഭിച്ചകാലം മുതൽ സ്കൂൾ വിദ്യാർത്ഥികൾക്ക് കമ്പ്യൂട്ടർ അനുബന്ധ ഉപകരണങ്ങളും ഇന്റർനെറ്റ് സൗകര്യവും ഫലപ്രദമായി ഉപയോഗിക്കുന്നത് സംബന്ധിച്ച വിവിധ തലങ്ങളിൽ നിർദ്ദേശങ്ങൾ നൽകിയിട്ടുണ്ട്. പ്രധാനപ്പെട്ടവ താഴെ നൽകുന്നു:

(1) വിദ്യാഭ്യാസ വകുപ്പ് ഹൈസ്കൂൾ ക്ലാസുകൾക്കായി തയ്യാറാക്കിയ വിവരവിനിമയ സാങ്കേതികവിദ്യ (ഐ.സി.ടി) പാഠപുസ്തകങ്ങളിൽ സൈബർ സുരക്ഷയുമായി ബന്ധപ്പെട്ട ഭാഗങ്ങൾ താഴെപ്പറയുംപ്രകാരം ഉൾപ്പെടുത്തിയിട്ടുണ്ട്.

- എട്ടാം ക്ലാസിലെ *'വിസ്മയലോകം വിരൽത്തുമ്പിൽ'* എന്ന അധ്യായത്തിൽ *'ഇന്റർനെറ്റ് ഉപയോഗിക്കുമ്പോൾ.....!'*, *'മൊബൈൽ ഫോൺ ഉപയോഗിക്കുമ്പോൾ'* എന്നീ ശീർഷകങ്ങളിൽ.
- ഒൻപതാം ക്ലാസിലെ *'കൈയെത്തും ദൂരെ അതിരില്ലാ ലോകം'* എന്ന അധ്യായത്തിൽ *'ഇ-മെയിൽ ഉപയോഗം ചില മുൻകരുതലുകൾ....'*, *'സൈബർ കുറ്റകൃത്യങ്ങൾ'* എന്നീ ശീർഷകങ്ങളിൽ.
- പത്താം ക്ലാസിലെ *'ഇന്റർനെറ്റ് പ്രവർത്തിക്കുന്നത്'*, എന്ന അധ്യായത്തിൽ *'നവ സാമൂഹിക മാധ്യമങ്ങൾ'*, *'സാമൂഹിക മാധ്യമങ്ങൾ ഉപയോഗിക്കുമ്പോൾ'*, *'ശ്ലീലവും അശ്ലീലവും'* എന്നീ ശീർഷകങ്ങൾ.

(2) സ്കൂളുകൾക്ക് ലഭ്യമാക്കിയ ബ്രോഡ്ബാൻഡ് ഇന്റർനെറ്റ് ഫലപ്രദമായി ഉപയോഗിക്കുന്നത് സംബന്ധിച്ച് 29.07.2008 ന് എൻ.ഇ.പി.(3) 82869/07 നമ്പർ പ്രകാരം പൊതുവിദ്യാഭ്യസ ഡയറക്ടർ സർക്കുലർ പുറപ്പെടുവിച്ചിട്ടുണ്ട്.

(3) സ്കൂളുകളിലേയും വിദ്യാഭ്യാസ ഓഫീസുകളിലേയും ലാപ്ടോപ്പ് കമ്പ്യൂട്ടർ ഉപയോഗം സംബന്ധിച്ച് 29.09.2009 ന് എൻ.ഇ.പി (3) 66500/2008 നമ്പർ പ്രകാരം പൊതുവിദ്യാഭ്യസ ഡയറക്ടർ സർക്കുലർ പുറപ്പെടുവിച്ചിട്ടുണ്ട്.

(4) ഡിജിറ്റൽ ഉള്ളടക്കം, ഡിജിറ്റൽ ലൈബ്രറികൾ തുടങ്ങിയവ എസ്.സി.ഇ.ആർ.ടി യോ, എസ്.സി.ഇ.ആർ.ടി നിർദ്ദേശിക്കുന്ന ഏജൻസികളോ അംഗീകരിച്ചശേഷം മാത്രം സ്കൂളുകളിൽ വിന്യസിക്കാവൂ എന്നും പ്രൊപ്രൈറ്ററി സോഫ്റ്റ്‌വെയറുകൾ സ്കൂളുകളിൽ വിന്യസിക്കരുതെന്നും കൂടെ നിഷ്കർഷിക്കുന്ന 06.01.2018-ലെ സ.ഉ(സാധാ) നം.97/2018/ പൊ.വി.വ നമ്പർ സർക്കാർ ഉത്തരവ്.

(5) പൊതുവിദ്യാഭ്യാസ സംരക്ഷണ യജ്ഞത്തിന്റെ ഭാഗമായുള്ള ഹൈടെക് സ്കൂൾ പദ്ധതിയിൽ ഉൾപ്പെടുത്തി സർക്കാർ, എയ്ഡഡ് ഹൈസ്കൂൾ, ഹയർസെക്കന്ററി-വൊക്കേഷണൽ ഹയർ സെക്കന്ററി സ്കൂളുകളിലെ ക്ലാസ് മുറികൾ ഹൈടെക് ആക്കുന്നതിന് നൽകുന്ന ഉപകരണങ്ങളും സൗകര്യങ്ങളും സേവനങ്ങളും കുട്ടികൾക്ക് പ്രയോജനപ്പെടുത്തുന്നതിന് സ.ഉ.(സാധാ) നം. 165/2018/പൊ.വി.വ. തീയതി 10.01.2018 പ്രകാരം സ്കൂളുകളും കൈറ്റും തമ്മിൽ പ്രത്യേക ധാരണാപത്രവും ഒപ്പിട്ടിട്ടുണ്ട്.

2. 'സൈബർ സേഫ്റ്റി ക്ലിനിക്കുകൾ'

പുതിയ കാലത്ത് സാങ്കേതിക വിദ്യകൾ അനവധി സാധ്യതകൾ വാഗ്ദാനം ചെയ്യുമ്പോഴും അവ മൂലമുണ്ടാകുന്ന ഭീഷണികളും കുറ്റകൃത്യങ്ങളും ഏറെക്കുറെ തുല്യ അളവിലാണ്. സൈബർ കുറ്റകൃത്യങ്ങളെക്കുറിച്ചുള്ള ബോധവൽക്കരണം പലപ്പോഴും ഉപദേശ ലഘുലേഖകളും പ്രസംഗങ്ങളും മാത്രമായി മാറിപ്പോകുന്ന സാഹചര്യമുണ്ട്. പലപ്പോഴും സൈബർ ഉപയോഗത്തിന് കടുത്ത നിയന്ത്രണങ്ങളാണ് ഇത്തരം ക്ലാസുകളിലും രേഖകളിലും നിഷ്കർഷിച്ച് വരാറുള്ളത്. ഇത് ഇത്തരം നൂതന സാങ്കേതിക വിദ്യകളെ ഫലപ്രദമായി പ്രയോജനപ്പെടുത്താനുള്ള സാധ്യതകളെക്കൂടെ ഇല്ലാതാക്കുകയോ അല്ലെങ്കിൽ അനാവശ്യ ഭീതി പടർത്തുകയോ ചെയ്യുന്നു എന്ന നിരീക്ഷണവുമുണ്ട്. ഈ സാഹചര്യത്തിൽ സൈബർ സുരക്ഷ ഉറപ്പാക്കാൻ ക്രിയാത്മകമായ ഇടപെടൽ ബഹുമുഖമായ തലത്തിൽ നടത്താൻ

കേരള ഇൻഫ്രാസ്ട്രക്ചർ ആൻഡ് ടെക്നോളജി ഫോർ എഡ്യൂക്കേഷൻ (കൈറ്റ്) തീരുമാനിച്ചിട്ടുണ്ട്. ഐ.സി.ടി പാഠപുസ്തകങ്ങൾ, സമഗ്ര പോർട്ടൽ എന്നിവയ്ക്ക് പുറമെ ലിറ്റിൽ കൈറ്റ്സ് ക്ലബ്ബുകളെ ഉപയോഗിച്ച് സൈബർ ചതിക്കുഴികൾ തിരിച്ചറിയാനും സൈബർ കുറ്റകൃത്യങ്ങളെ പ്രതിരോധിക്കാനും പരിഹാരം കാണാനും ഇന്ററാക്ടീവ് ഗെയിമുകൾ ഉൾപ്പെടെ എഡ്യൂടെയിൻമെന്റ് മാതൃകയിൽ വളരെ വിപുലമായ പദ്ധതി 2019-20 അധ്യയനവർഷം മുതൽ നടപ്പാക്കുന്നതാണ്. ഐ.ഒ.ടി, റോബോട്ടിക്സ്, 3D ക്യാരക്ടർ അനിമേഷൻ തുടങ്ങിയ മേഖലകളിൽ ലിറ്റിൽ കൈറ്റ്സ് അംഗങ്ങൾക്കുള്ള വിദഗ്ധ പരിശീലനം വിജയകരമായി പൂർത്തിയാക്കിയ അനുഭവത്തിൽ ഇനി സ്കൂളുകളിൽ 'സൈബർ സേഫ്റ്റി ക്ലിനിക്കുകൾ' സ്ഥാപിക്കൽ ഇതിന്റെ ഭാഗമായ പ്രധാന പ്രവർത്തനമാണ്. അധ്യാപകർക്കും ഈ മേഖലയിൽ പരിശീലനം നൽകുന്നതോടൊപ്പം രക്ഷിതാക്കൾക്കും സൈബർ സുരക്ഷയിൽ പ്രായോഗിക പരിശീലനം ഇതിന്റെ ഭാഗമായി നൽകും. ഇന്ററാക്ടീവ് ഗെയിമുകളിലൂടെ കാര്യങ്ങൾ വളരെയെളുപ്പം മനസിലാക്കാവുന്ന രൂപത്തിൽ സാങ്കേതിക സങ്കീർണതകൾ ഒഴിവാക്കിയും സാഹചര്യങ്ങളെ പുനഃസൃഷ്ടിച്ചുമാണ് ഇത്തരം പരിശീലനങ്ങൾ നടത്തുക. അതോടൊപ്പം സാങ്കേതിക വിദ്യകളുടെ സാധ്യതകളെ ഫലപ്രദമായി അവതരിപ്പിക്കുകയും ചെയ്യും. ഇതിനായി ഈ മേഖലയിൽ വൈദഗ്ധ്യവും വിശ്വാസ്യതയുമുള്ള സ്ഥാപനങ്ങളുടേയും വ്യക്തികളുടേയു മെല്ലാം സേവനം കൈറ്റ് പ്രയോജനപ്പെടുത്തും.

സ്കൂൾ കുട്ടികൾക്കുവേണ്ടിയുള്ള സൈബർ സേഫ്റ്റി പ്രോട്ടോക്കോൾ വിവിധ തലങ്ങളിൽ നടപ്പിലാക്കുന്നതിനുള്ള നിർദ്ദേശങ്ങൾ ചുവടെ ചേർക്കുന്നു:

3. ഓഫീസ് മേധാവി ഉറപ്പുവരുത്തേണ്ട കാര്യങ്ങൾ

(1) വിദ്യാലയങ്ങളിൽ ലഭ്യമാക്കിയിട്ടുള്ള ഇന്റർനെറ്റ് സംവിധാനം തടസ്സം കൂടാതെ അധ്യാപകർക്കും കുട്ടികൾക്കും ലഭ്യമാക്കൽ സ്കൂൾ മേലധികാരിയുടെ ഉത്തരവാദിത്തമാണ്. ആയതിനാൽ പ്രവൃത്തി സമയങ്ങളിൽ വിദ്യാഭ്യാസ ആവശ്യങ്ങൾക്ക് കുട്ടികൾക്ക് ഇന്റർനെറ്റ് ലഭ്യത ഉറപ്പാക്കേണ്ടതാണ്.

(2) സ്കൂൾ ലാബുകളിൽ ഉപയോഗിക്കുന്ന ഐ.ടി ഉപകരണങ്ങളിൽ സുരക്ഷാ ക്രമീകരണം ഒരുക്കേണ്ടതും സ്കൂൾ ഐടി കോർഡിനേറ്റർ, അതത് ക്ലാസ് അധ്യാപകർ/ പ്രഥമാധ്യാപകർ തുടങ്ങിയവർ ഇത് ഉറപ്പുവരുത്തേണ്ടതുമാണ്.

(3) കുട്ടികളുടെ ഇന്റർനെറ്റ് ഉപയോഗം അധ്യാപകരുടെ നിരീക്ഷണത്തിലായിരിക്കണം. ഇന്റർനെറ്റ് ലഭ്യമാക്കുന്ന സ്ഥലങ്ങളിലും ലാബുകളിലും ഇരിപ്പിടം അതിനനുസൃതമായി ക്രമീകരിക്കേണ്ടതാണ്.

(4) വിദ്യാലയങ്ങളിൽ ലഭ്യമാക്കിയിട്ടുള്ള ഇന്റർനെറ്റ് സംവിധാനം പാസ്‌വേഡ് ഉപയോഗിച്ച് സുരക്ഷിതമാക്കേണ്ടതാണ്.

(5) ആവശ്യമെങ്കിൽ 'restricted mode', 'safesearch', 'supervised users' തുടങ്ങിയ ഫിൽറ്ററുകളും സംവിധാനങ്ങളും കുട്ടികളുടെ സുരക്ഷിതമായ ഇന്റർനെറ്റുപയോഗത്തിന് പ്രയോഗിക്കേണ്ടതാണ്. ഇക്കാര്യത്തിൽ ആവശ്യമായ പരിശീലനം അധ്യാപകർക്ക് ലഭിച്ചു എന്നുറപ്പാക്കേണ്ടതാണ്.

(6) ലാബുകളിലും ക്ലാസുകളിലും ഇന്റർനെറ്റ് ആവശ്യമുള്ള സമയങ്ങളിൽ മാത്രം ഉപയോഗിക്കുന്നുവെന്ന് ഉറപ്പുവരുത്തേണ്ടതാണ്. വിദ്യാലയ പ്രവൃത്തി സമയങ്ങൾക്കുപരിയായി ഇന്റർനെറ്റ് സംവിധാനം ഉപയോഗിക്കേണ്ടിവന്നാൽ സ്കൂൾ അധികൃതരുടെ അറിവും അനുവാദവും ഉറപ്പുവരുത്തേണ്ടതാണ്. ഇന്റർനെറ്റ് ഉപയോഗശേഷം കൃത്യമായി ഇന്റർനെറ്റ് സ്വിച്ച് ഓഫ് ചെയ്ത് കമ്പ്യൂട്ടർ ഷട്ട്ഡൗൺ ചെയ്തുവെന്ന് അനുമതി നൽകുന്നവർ ഉറപ്പുവരുത്തേണ്ടതാണ്.

(7) ഇന്റർനെറ്റ് ശരിയായി ഉപയോഗിക്കുന്നത് സംബന്ധിച്ച സന്ദേശങ്ങൾ, നിർദ്ദേശങ്ങൾ തുടങ്ങിയവ ക്ലാസുകളിലും ലാബുകളിലും പ്രദർശിപ്പിച്ചിരിക്കണം.

(8) ആമുഖത്തിൽ (1(1)) സൂചിപ്പിച്ച 8, 9, 10 ക്ലാസുകളിലെ ഐ.സി.ടി പാഠപുസ്തകങ്ങളിൽ സൈബർ സുരക്ഷയുമായി ബന്ധപ്പെട്ട് നൽകിയ കാര്യങ്ങൾ പ്രത്യേകം ചർച്ച ചെയ്യാൻ സ്കൂളുകളിൽ സംവിധാനം ഒരുക്കേണ്ടതാണ്.

(9) പൊതുവായി ഇന്റർനെറ്റ് ഉപയോഗിക്കുന്നതിന് നൽകുന്ന കമ്പ്യൂട്ടർ പാസ്‌വേഡ് ഉപയോഗിച്ച് സുരക്ഷിതമാക്കേണ്ടതാണ്. വിദ്യാലയം ഉപയോഗിക്കുന്ന എല്ലാ ഓൺ ലൈൻ, ഓഫ് ലൈൻ സോഫ്റ്റ്‌വെയറും കൃത്യമായി പാസ്‌വേഡ് ഉപയോഗിച്ച് സുരക്ഷിതമാക്കേണ്ടതും സോഫ്റ്റ്‌വെയറിന്റെ ചുമതലയുള്ളവർക്കുമാത്രം അതത് പാസ് വേഡ് ലഭ്യമാക്കുന്നതിന് ക്രമീകരണം ഒരുക്കേണ്ടതുമാണ്.

(10) ആമുഖം (1(4)) ഉത്തരവിൽ പരാമർശിച്ചപ്രകാരം ഉടമസ്ഥാവകാശമുള്ള സോഫ്റ്റ് വെയറുകൾ, പൈറേറ്റഡ് പകർപ്പുകൾ എന്നിവ സ്കൂളിലെ കമ്പ്യൂട്ടറുകളിൽ ഇല്ല എന്നുറപ്പാക്കേണ്ട താണ്.

(11) സ്കൂളുകളിൽ വർഷത്തിൽ രണ്ട് തവണയെങ്കിലും 'സൈബർ സേഫ്റ്റി ഓഡിറ്റ്' നടത്തേണ്ടതാണ്. (ഇതിനായുള്ള മാർഗനിർദ്ദേശങ്ങൾ പ്രത്യേകം ലഭ്യമാക്കുന്നതാണ്.)

4. അധ്യാപകർ ഉറപ്പുവരുത്തേണ്ടത്

(1) കുട്ടികളുടെ സാന്നിധ്യത്തിൽ ഇന്റർനെറ്റിൽ നിന്ന് വിഭവങ്ങൾ ശേഖരിക്കുന്നത് അനുയോജ്യമല്ലാത്ത വിഭവങ്ങൾ പ്രദർശിപ്പിക്കപ്പെടുന്നതിന് ഇടയായേക്കാം. അതിനാൽ അധ്യാപകർ ക്ലാസിൽ ഉപയോഗിക്കേണ്ട ഐസിടി ബോധന സഹായികൾ (ഇന്റർനെറ്റിൽ നിന്ന് ശേഖരിക്കേണ്ടതാണെങ്കിൽ) മുൻകൂട്ടി തയ്യാറാക്കി ക്ലാസിൽ അവതരിപ്പിക്കേണ്ടതാണ്.

(2) ക്ലാസിൽ അധ്യാപകർ നേരിട്ട് ഇന്റർനെറ്റിൽ നിന്ന് വിഭവങ്ങൾ അന്വേഷിച്ച് കണ്ടെത്തുന്നത് ഒഴിവാക്കുന്നതിനായി വിദ്യാഭ്യാസവകുപ്പ് തയ്യാറാക്കിയ സമഗ്ര റിസോഴ്സ് പോർട്ടലിൽ നിന്നുള്ള വിവരങ്ങൾ ക്ലാസിൽ പരമാവധി ഉപയോഗിക്കേണ്ടതാണ്.

(3) കുട്ടികൾക്ക് ഇന്റർനെറ്റ് അധിഷ്ഠിത പഠന പ്രോജക്റ്റുകൾ നൽകുമ്പോൾ പരിശോധിച്ച് ഉറപ്പുവരുത്തിയ റഫറൻസ് സൈറ്റുകൾ മാത്രം നിർദേശിക്കണം.

(4) അധ്യാപകരുടേയോ മറ്റ് ചുമതലയുള്ളവരുടെയോ മേൽനോട്ടത്തിൽ മാത്രം കുട്ടികൾ ക്ക് ഇന്റർനെറ്റ് ഉപയോഗിക്കാൻ അവസരം നൽകേണ്ടതാണ്.

(5) സ്കൂളിലെ ഇന്റർനെറ്റ് ഉപയോഗം പഠനാവശ്യങ്ങൾക്കും ഔദ്യോഗിക ആവശ്യങ്ങൾക്കും മറ്റ് പഠനാനുബന്ധ പ്രവർത്തനങ്ങൾക്കും മാത്രമായി പരിമിതപ്പെടുത്തേണ്ടതാണ്.

(6) ഇന്റർനെറ്റ് അധിഷ്ഠിതമായ പ്രവർത്തനങ്ങൾ ക്ലാസ്സ്റൂം ഗ്രൂപ്പുകളിൽ ചെയ്യുമ്പോൾ പ്രവർത്തനങ്ങൾ മുൻകൂട്ടി ആസൂത്രണം ചെയ്യുകയും കുട്ടികൾ ആ പ്രവർത്തനങ്ങൾ വിട്ട് മറ്റുള്ളവയിലേക്ക് പോകുന്നതിനുള്ള അവസരങ്ങൾ ഉണ്ടാകാതെ നോക്കുകയും വേണം.

5. വിദ്യാർത്ഥികൾ പാലിക്കേണ്ട കാര്യങ്ങൾ

(1) അധ്യാപകരുടെ നിർദ്ദേശാനുസരണം മാത്രമായിരിക്കണം വിദ്യാലയങ്ങളിൽ ഇന്റർ നെറ്റ് ഉപയോഗിക്കേണ്ടത്.

(2) വിശ്വസനീയമല്ലാത്ത കേന്ദ്രങ്ങളിൽനിന്നോ വെബ്സൈറ്റുകളിൽ നിന്നോ ലഭിക്കുന്ന ആപ്ലിക്കേഷനുകൾ ഡൗൺലോഡ് ചെയ്യുകയോ, ഇൻസ്റ്റാൾ ചെയ്ത് ഉപയോഗിക്കുകയോ ചെയ്യരുത്.

(3) വിദ്യാലയങ്ങൾ, ഓഫീസുകൾ തുടങ്ങി പൊതുഇടങ്ങളിൽ ഉപയോഗിക്കുന്ന കമ്പ്യൂട്ടറുകളിൽ വ്യക്തിഗത വിവരങ്ങളോ, ചിത്രങ്ങളോ സൂക്ഷിക്കരുത്. ചിത്രങ്ങൾമോർ

ഫ് ചെയ്യും മറ്റുമെല്ലാം ദുരുപയോഗം ചെയ്യപ്പെടാം. മറ്റുള്ള കുട്ടികളുടെ (വ്യക്തികളുടെ) വിവരങ്ങൾ ഇപ്രകാരം ദുരുപയോഗം ചെയ്യരുത്.

(4) മൊബൈൽ ഫോൺ, ലാപ്ടോപ്പ് എന്നിവ അപരിചിതരെ ഏൽപിക്കരുത്.

(5) കുട്ടികൾ അവരുടെ സ്വകാര്യ വിവരങ്ങൾ അപരിചിതരുമായി ഇന്റർനെറ്റിൽ/ സോഷ്യൽമീഡിയയിൽ പങ്കുവെയ്ക്കരുത്. ഓൺലൈൻ പരിചയം മാത്രമുള്ളവരെ രക്ഷിതാക്കളുടെയോ മറ്റോ കൂടെയല്ലാതെ ഒരിക്കലും നേരിട്ട് കാണാൻ ശ്രമിക്കരുത്. പരിചയമില്ലാത്തതോ, വിശ്വാസമില്ലാത്തതോ ആയ ആളുകൾ അയയ്ക്കുന്ന സന്ദേശങ്ങൾ (ഇ-മെയിലുകൾ) തുറക്കരുത്.

(6) രക്ഷിതാക്കളുടേയോ മറ്റുള്ളവരുടേയോ ക്രെഡിറ്റ്/ഡെബിറ്റ് കാർഡിന്റെ പിൻ കോഡ്, പാസ്‌വേഡ്, ഓൺലൈൻ ബാങ്ക് അക്കൗണ്ട് പാസ്‌വേഡ് തുടങ്ങിയവ ശേഖരിക്കുകയോ മറ്റുള്ളവർക്ക് കൈമാറുകയോ ചെയ്യരുത്.

(7) ഓൺലൈൻ ഗെയിമുകളിൽ വളരെ ശ്രദ്ധാപൂർവ്വം ഇടപെടുക. പലപ്പോഴും ഇത്തരം ഗെയിമുകൾക്ക് അടിമപ്പെടുന്ന അവസ്ഥവരെ ഉണ്ടാകും. പലതരം വെല്ലുവിളികൾ ഏറ്റെടുക്കൽ, സ്വകാര്യ വിവരങ്ങളും ചിത്രങ്ങളും ആവശ്യപ്പെടൽ തുടങ്ങിയ ആവശ്യങ്ങൾക്ക് ഒരിക്കലും വഴങ്ങാതിരിക്കുക.

(8) സൈബർ സ്പേസിൽ പ്രധാനമായും കുട്ടികളെ ലക്ഷ്യമിട്ടുകൊണ്ടുള്ള നിരവധി കുറ്റകൃത്യങ്ങൾ (സൈബർ ക്രൈമുകൾ നടക്കുന്നുണ്ട്. അവയിൽ പ്രധാനപ്പെട്ട ചിലത് താഴെ നൽകുന്നു:

*i. **ഫിഷിംഗ് (Phishing):** യഥാർത്ഥ സ്രോതസിൽ നിന്ന് എന്ന ധാരണ പരത്തുന്നവിധം വ്യാജ ഇ-മെയിലുകളിൽ നിന്നും, മൊബൈൽ ഫോൺ, ഫെയ്സ്ബുക്ക് തുടങ്ങിയ അക്കൗണ്ടുകളിൽ നിന്നും സന്ദേശം ലഭിക്കുക. നിങ്ങൾക്ക് ലോട്ടറി അടിച്ചു, അവാർഡ് ലഭിച്ചു, ജോലി ലഭിച്ചു എന്നൊക്കെ സൂചിപ്പിച്ചു വരുന്ന സന്ദേശങ്ങൾ ഈ വിഭാഗത്തിലുള്ളവയാണ. ബാങ്ക് അക്കൗണ്ട് ഉൾപ്പെടെയുള്ള വിവരങ്ങൾ ചോർത്തി തട്ടിപ്പ നടത്തുകയാണ് ഉദ്ദേശം. അയയ്ക്കുന്ന വ്യക്തിയുടെ യഥാർത്ഥ വിലാസം (അക്കൗണ്ട്) മറച്ചുവെക്കുന്ന സ്പൂഫിംഗ് (Spoofing) ഇതിന്റെ മറ്റൊരു രൂപമാണ്.*

*ii. **സൈബർ സ്റ്റാക്കിംഗ് (Cyber Stalking):** നമ്മെക്കുറിച്ചുള്ള വിവരങ്ങൾ സോഷ്യൽ മീഡിയ വഴിയോ മറ്റോ ഒക്കെ ശേഖരിച്ച് ഭീഷണിപ്പെടുത്തിയും, ബ്ലാക്ക്മെയിൽ ചെയ്തുമെല്ലാം ഉപദ്രവിക്കുക.*

*iii. **ഡീപ്ഫെയ്ക്സ് (Deepfakes):** ഒരു ചിത്രത്തിൽ അല്ലെങ്കിൽ വീഡിയോയിൽ ചിത്രവും ശബ്ദവും ചലനങ്ങളുമെല്ലാം മാറ്റി ഒറിജിലിനെ വെല്ലുന്ന വ്യാജൻ നിർമ്മിക്കുക. പെട്ടെന്ന് തിരിച്ചറിയാൻ കഴിയാത്ത രൂപത്തിലാകും ഇവ. അതിനാൽ ആധികാരികത ഉറപ്പാക്കാത്ത വീഡിയോകൾ-ചിത്രങ്ങൾ-വോയ്സ് ക്ലിപ്പുകൾ മറ്റൊരാൾക്ക് ഫോർവേർഡ് ചെയ്യരുത.*

*iv. **ക്യാമറ ഹാക്കിംഗ് (Camera Hacking):** അംഗീകാരമില്ലാത്ത കമ്പ്യൂട്ടർ/ഐടി സംവിധാനങ്ങളിൽ നുഴഞ്ഞു കയറുന്നതാണ് പൊതുവെ ക്രാക്കിംഗ്' എന്ന് വിശേഷിപ്പിക്കാറുള്ളത്. (യഥാർത്ഥത്തിൽ ഇത്തരം നശീകരണ ഉദ്ദേശ്യത്തോടെ യുള്ള നുഴഞ്ഞു കയറൽ ഹാക്കിംഗ് ആണ്). ഇതുതന്നെ നമ്മുടെ*

ലാപ്ടോപ്പിലെയോ, മൊബൈലിലെയോ ക്യാമറ ഉപയോഗിച്ച് നമ്മുടെ അനുവാദമില്ലാതെതന്നെ സ്വകാര്യ ചിത്രങ്ങളും വീഡിയോകളും എടുക്കാൻ കഴിയുന്നതാണ് ക്യാമറ ഹാക്കിംഗ്. അതായത, നാം ക്യാമറ ഉപയോഗിക്കുമ്പോൾ മാത്രമല്ല, നാമറിയാതെ നമ്മുടെ ഉപകരണത്തിന്റെ ക്യാമറ പ്രവർത്തിപ്പിക്കാൻ വരെ ക്രാക്കർമാർക്ക് കഴിയും. ഇത് സാധ്യമാക്കുന്നത് നാം ശ്രദ്ധിക്കാതെപോലും ഡൗൺലോഡ് ചെയ്യുന്ന ചില നശീകരണകാരികളായ പ്രോഗ്രാമുകൾ (വൈറസുകൾ, മാൽവെയറുകൾ)

വഴിയാണ് എന്നതിനാൽ വ്യക്തമായ ധാരണ ഇല്ലാത്ത ആപ്പുകളും അറ്റാച്ചമെന്റുകളും ഡൗൺലോഡ് ചെയ്യാതിരിക്കാൻ പ്രത്യേകം ശ്രദ്ധിക്കുക.

(ആമുഖം 1(1) ൽ പരാമർശിച്ച പാഠപുസ്തകങ്ങളിൽ നൽകിയിട്ടുള്ള മറ്റ് സൈബർ കുറ്റകൃത്യങ്ങൾ കൂടി കാണുക)

(9) ഓൺലൈനിൽ പോസ്റ്റ് ചെയ്യുന്ന വിവരങ്ങൾ അവിടെ നിന്നും മാഞ്ഞുപോകില്ല എന്നതിനാൽ പലവട്ടം ആലോചിച്ചുറപ്പിച്ചതിന് ശേഷം മാത്രം വിവരങ്ങൾ നൽകുക. അശ്ലീല ചിത്രങ്ങൾ കൈമാറുന്ന 'സെക്സ്റ്റിംഗ്' ഉൾപ്പെടെ സൈബർ കുറ്റകൃത്യങ്ങളുടെ ഗണത്തിൽപ്പെടുന്നതും ഇന്ത്യൻ സൈബർ നിയമപ്രകാരം ശിക്ഷാർഹവുമാണ് എന്നോർക്കുക.

(10) സൈബർ നിയമപ്രകാരം കുറ്റകരമായ രൂപത്തിൽ സ്വന്തമായി സന്ദേശങ്ങൾ തയ്യാറാക്കുന്നതും 'ട്രോളുകൾ' സൃഷ്ടിക്കുന്നതും മാത്രമല്ല മറ്റൊരാൾ തയ്യാറാക്കിയ വസ്തുതാവിരുദ്ധവും, ഹാനികരവുമായ സന്ദേശങ്ങൾ, ചിത്രങ്ങൾ, വീഡിയോകൾ തുടങ്ങിയവ ഫോർവേർഡ് ചെയ്യുന്നതും സൈബർ നിയമപ്രകാരം കുറ്റകരമാണ് എന്നോർക്കുക.

(11) സൈബർ ഉപയോഗവുമായി ബന്ധപ്പെട്ട് ഉണ്ടാകുന്ന ബുദ്ധിമുട്ടുകൾ, ഭീഷണികൾ തുടങ്ങിയവ രക്ഷിതാക്കളുമായും അധ്യാപകരുമായും തുറന്ന് സംസാരിക്കുക.

6. രക്ഷിതാക്കൾ ശ്രദ്ധിക്കേണ്ട കാര്യങ്ങൾ

1) ക്രെഡിറ്റ്/ഡബിറ്റ് കാർഡിന്റെ പിൻ കോഡ്, പാസ്‌വേഡ്, ഓൺ ലൈൻ ബാങ്ക് അക്കൗണ്ട് പാസ്‌വേർഡ് തുടങ്ങിയവ കുട്ടികൾക്ക് നൽകാൻ പാടില്ല.

2) വിദ്യാലയങ്ങളിലെ ഉപയോഗത്തിന് സ്കൂൾ നിർദ്ദേശിക്കുന്നതല്ലാത്ത ഉപകരണങ്ങൾ കുട്ടിക്ക് നൽകരുത്.

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

4) സാങ്കേതിക വിദ്യകളുടെ ഉപയോഗം മനസിലാക്കാൻ ശ്രമിക്കുക. നിങ്ങളുടെ അറിവ് പുതുക്കിക്കൊണ്ടിരിക്കുക. സാമൂഹ്യ മാധ്യമങ്ങളും മറ്റും ഉപയോഗിക്കുന്നതിനെക്കുറിച്ച് കുട്ടികളുമായി തുറന്ന് ചർച്ച ചെയ്യുക.

5) സാങ്കേതിക സംവിധാനങ്ങളുടെ (ഇന്റർനെറ്റ്, മൊബൈൽ ഫോൺ) അമിത ഉപയോഗം കുട്ടികളിലുണ്ടോ എന്ന് നിരീക്ഷിക്കുക. കുട്ടിയിൽ എന്തെങ്കിലും തരത്തിലുള്ള പെരുമാറ്റ വൈകല്യങ്ങളുടെ സൂചനയോ ലക്ഷണങ്ങളോ കാണുകയോ സൈബർ കുറ്റകൃത്യങ്ങൾക്ക് അവർ ഇരയായെന്ന് അറിയുകയോ ചെയ്താൽ കുട്ടികളോട് തുറന്ന് സംസാരിക്കുക. കൂടുതൽ ഭയപ്പെടുത്താതെ കാര്യങ്ങൾ വിശദമായി ചോദിച്ചറിയുകയും, ആവശ്യമായ തെളിവുകൾ ശേഖരിക്കുകയും ചെയ്യുക. ബന്ധപ്പെട്ട ഉദ്യോഗസ്ഥരോട് പരാതിപ്പെടാനും ആവശ്യമെങ്കിൽ കൗൺസിലിംഗ് നൽകാനും ശ്രദ്ധിക്കുക.

7. പൊതുനിർദ്ദേശങ്ങൾ

1) ഇന്റർനെറ്റ് ഉപയോഗം സംബന്ധിച്ച സന്ദേശങ്ങൾ, നിർദ്ദേശങ്ങൾ തുടങ്ങിയവ ക്ലാസുകളിലും ലാബുകളിലും പ്രദർശിപ്പിച്ചിരിക്കണം.

2) അപരിചിതരിൽ നിന്ന് മൊബൈൽ ഫോൺ, ക്യാമറ, ഐപാഡ് തുടങ്ങിയ ഉപകരണങ്ങൾ സ്വീകരിക്കുകയോ കൈമാറുകയോ ചെയ്യരുത്.

3) വ്യക്തികളുടേയോ സ്ഥാപനങ്ങളുടേയോ ചിത്രങ്ങൾ അനുവാദം ഇല്ലാതെ ചിത്രീകരിക്കുകയോ പ്രചരിപ്പിക്കുകയോ അരുത്.

4) നിങ്ങളുടെ ഫോൺകോളുകളോ സന്ദേശങ്ങളോ സ്വീകരിക്കാൻ താൽപര്യമില്ലാത്ത ഒരാളെ നിരന്തരം വിളിക്കുകയോ സന്ദേശങ്ങൾ അയക്കുകയോ ചെയ്യരുത്.

5) വിശ്വസനിയമല്ലാത്ത കേന്ദ്രങ്ങളിൽ നിന്നോ വെബ്സൈറ്റുകളിൽ നിന്നോ ലഭിക്കുന്ന ആപ്ലിക്കേഷനുകൾ ഡൗൺലോഡ് ചെയ്യുകയോ, ഇൻസ്റ്റാൾ ചെയ്ത് ഉപയോഗിക്കുകയോ ചെയ്യരുത്.

6) അപരിചിതമായ നമ്പറുകളിൽ നിന്നും തുടർച്ചയായി മിസ്ഡ് കോളുകൾ വരികയാണെങ്കിൽ അധ്യാപകരേയോ രക്ഷിതാക്കളേയോ അറിയിക്കണം.

7) അനധികൃതമായി നിങ്ങളുടെ ഫോട്ടോ എടുക്കുന്നതായി ശ്രദ്ധയിൽപെട്ടാൽ അധ്യാപകരേയോ രക്ഷിതാക്കളേയോ അറിയിക്കേണ്ടതാണ്.

8) സൈബർ സുരക്ഷയുമായി ബന്ധപ്പെട്ട കാര്യങ്ങൾക്ക് കേരളാ പോലീസിന്റെ ഫോൺ നമ്പറും (1090) ചൈൽഡ് ഹെൽപ് ലൈൻ നമ്പറും (1098) ആവശ്യഘട്ടങ്ങളിൽ ഉപയോഗിക്കേണ്ടതാണ്.

9) ഇന്റർനെറ്റിന്റെയും സോഷ്യൽമീഡിയയുടെയും ഫലപ്രദമായ ഉപയോഗം സംബന്ധിച്ച മൊഡ്യൂൾ അധ്യാപക പരിശീലനങ്ങളിൽ ഉൾപ്പെടുത്തേണ്ടതാണ്. കൈറ്റ് വിക്ടേഴ്സ് ചാനൽ വഴിയും പൊതുവിദ്യാഭ്യാസ വകുപ്പിന്റെ മറ്റു വെബ് പോർട്ടലുകൾ വഴിയും ബോധവൽക്കരണ വീഡിയോകൾ ലഭ്യമാക്കേണ്ട താണ്.

10) ഇന്റർനെറ്റ് ഉപയോഗം സംബന്ധിച്ച് കുട്ടികൾക്കുള്ള ബോധവൽക്കരണ ക്ലാസുകൾ 'ലിറ്റിൽ കൈറ്റ്സ് ' യൂണിറ്റിന്റേയോ സ്കൂൾ ക്ലബ്ബുകളുടെയോ നേതൃത്വത്തിൽ നിശ്ചിത ഇടവേളകളിൽ ക്രമീകരിക്കേണ്ടതാണ്.

11) സ്കൂളുകളിൽ സൈബർ സേഫ്റ്റി ക്ലിനിക്കുകൾ സ്ഥാപിക്കുന്നതുമായി ബന്ധപ്പെട്ട് പ്രത്യേകം വിശദാംശങ്ങൾ പുറപ്പെടുവിക്കേണ്ടതാണ്.

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

കെ. അൻവർ സാദത്ത്
വൈസ് ചെയർമാൻ & എക്സിക്യൂട്ടീവ് ഡയറക്ടർ
കേരള ഇൻഫ്രാസ്ട്രക്ചർ & ടെക്നോളജി ഫോർ എഡ്യൂക്കേഷൻ (കൈറ്റ്)
ഇ-മെയിൽ : contact@kite.kerala.gov.in