ಕರ್ನಾಟಕ ಸರ್ಕಾರ

ಸಮಗ್ರ ಮಕ್ಕಳ ರಕ್ಷಣಾ ಯೋಜನೆ

C/o ನಿರ್ದೇಶನಾಲಯ, ಮಹಿಳಾ ಮತ್ತು ಮಕ್ಕಳ ಅಭಿವೃದ್ಧಿ ಇಲಾಖೆ, ಒಂದನೇ ಮಹಡಿ, ಬಹು ಮಹಡಿಗಳ ಕಟ್ಟಡ, ಡಾ॥ಬಿ.ಆರ್. ಅಂಬೇಡ್ಕರ್ ವೀದಿ, ಬೆಂಗಳೂರು-560 001, ಕರ್ನಾಟಕ

E-mail ID:icpc.kar@gmail.com
Phone No: 080-22879381

ಸಂಖ್ಯೆ:ಕೆಎಸ್‌ಐಸಿಪಿಎಸ್/ಐಇಸಿ/Online Safety /11/2020-21
ದಿನಾಂಕ:10-08-2020

ಜಿಲ್ಲಾ ಮಕ್ಕಳ ರಕ್ಷಣಾಧಿಕಾರಿಗಳು,
ಜಿಲ್ಲಾ ಮಕ್ಕಳ ರಕ್ಷಣಾ ಘಟಕ,
ಎಲ್ಲಾ ಜಿಲ್ಲೆಗಳು.

ವಿಷಯ: ಮಕ್ಕಳಿಗೆ, ಪೋಷಕರಿಗೆ, ಹದಿಹರೆಯದ ಮಕ್ಕಳಿಗೆ, ಶಾಲಾ ಶಿಕ್ಷಕರಿಗೆ ಹಾಗೂ ಸಾರ್ವಜನಿಕರಿಗೆ Online Safety ಕುರಿತಂತೆ ಮುಖ್ಯವಾಗಿ Online Child Porn ವಿರುದ್ಧ ಅರಿವು ಮೂಡಿಸುವ ಕಾರ್ಯಕ್ರಮಗಳನ್ನು ಆಯೋಜಿಸುವ ಬಗ್ಗೆ.

****

ಮೇಲಿನ ವಿಷಯಕ್ಕೆ ಸಂಬಂಧಿಸಿದಂತೆ, ಇತ್ತೀಚಿನ ದಿನಗಳಲ್ಲಿ ಮನರಂಜನೆ, ಜಾಹೀರಾತು ಹಾಗೂ ಯಾವುದೇ ವಿಷಯ ವಿಶ್ಲೇಷಣೆಗೆ ಸಾಮಾಜಿಕ ಜಾಲತಾಣ (Internet) ಬಳಸುವುದು ಸಾಮಾನ್ಯವಾಗಿದೆ. ಸಾಮಾಜಿಕ ಜಾಲತಾಣ ಬಳಸುವವರಿಗೆ ಇದರ ಕುರಿತ ಅನುಕೂಲ/ಅನಾನುಕೂಲಗಳ ಬಗ್ಗೆ ಮಾಹಿತಿ ಇರುವುದು ಹಾಗೂ ಬಳಸುವ ರೀತಿಯ ಕುರಿತು ಮಾಹಿತಿ ಇರುವುದು ಅತ್ಯಾವಶ್ಯಕವಾಗಿದೆ.

ಮಕ್ಕಳ ರಕ್ಷಣೆ ನಮ್ಮ ಆದ್ಯ ಕರ್ತವ್ಯವಾಗಿರುತ್ತದೆ. ಇತ್ತೀಚಿನ ದಿನಗಳಲ್ಲಿ ಮಕ್ಕಳಲ್ಲಿ Online, Digital ಮಾಧ್ಯಮ, ಸೈಬರ್ ಬಳಕೆ ಹೆಚ್ಚಾಗುತ್ತಿದ್ದು ಇದರಿಂದ ಮಕ್ಕಳನ್ನು ರಕ್ಷಿಸಬೇಕಾಗುತ್ತದೆ. ಸುರಕ್ಷಿತವಾಗಿ ಸಾಮಾಜಿಕ ಜಾಲತಾಣಗಳನ್ನು ಬಳಕೆ ಮಾಡುವಂತೆ ಮಾಡಬೇಕಾದ ಜವಾಬ್ದಾರಿ ಪಾಲಕರು, ಶಿಕ್ಷಕರು ಹಾಗೂ ಸಾರ್ವಜನಿಕರದಾಗಿರುತ್ತದೆ. ಇದಕ್ಕೆ ಸಂಬಂಧಿಸಿದಂತೆ ಐಸಿಪಿಎಸ್ ವತಿಯಿಂದ Online Safety ಕುರಿತಂತೆ ಮುಖ್ಯವಾಗಿ Online Child Porn ವಿರುದ್ಧವಾಗಿ 1.ಮಕ್ಕಳಿಗೆ, 2.ಪೋಷಕರಿಗೆ, 3.ಹದಿಹರೆಯದ ಹಾಗೂ 4.ಶಿಕ್ಷಕರಿಗೆ ಉಪಯುಕ್ತವಾಗುವಂತೆ ಡಾಕ್ಯುಮೆಂಟ್ಸ್ ಸಿದ್ಧಪಡಿಸಲಾಗಿದೆ.

ಈ ವಿಷಯಕ್ಕೆ ಸಂಬಂಧಿಸಿದಂತೆ ಶಾಲಾ ಮಕ್ಕಳಿಗೆ ಹಾಗೂ ಪದವಿ ಪೂರ್ವ ಕಾಲೇಜು ವಿದ್ಯಾರ್ಥಿಗಳಿಗೆ ಅರಿವು ಮೂಡಿಸುವ ಅಗತ್ಯವಿರುವುದರಿಂದ Online ಮೂಲಕ ಚರ್ಚೆಗಳು, ಸೆಮಿನಾರ್‌ಗಳನ್ನು ಆಯೋಜಿಸುವುದು ಹಾಗೂ ಸದರಿ ಕಾರ್ಯಕ್ರಮಗಳನ್ನು ಕೈಗೊಂಡಿರುವ ಕುರಿತ ವರದಿಯನ್ನು 10 ದಿನದ ಒಳಗಡೆ ಈ-ಮೇಲ್ ಮುಖಾಂತರ ಪ್ರಧಾನ ಕಛೇರಿಗೆ ಸಲ್ಲಿಸಲು ಕೋರಲಾಗಿದೆ. (Online Safety ಕುರಿತ ಡಾಕ್ಯುಮೆಂಟ್‌ಗಳನ್ನು ಲಗತ್ತಿಸಿದೆ).

ತಮ್ಮ ವಿಶ್ವಾಸಿ

10. 08. 2020

ನಿರ್ದೇಶಕರು,
ಸಮಗ್ರ ಮಕ್ಕಳ ರಕ್ಷಣಾ ಯೋಜನೆ,
ಬೆಂಗಳೂರು

ONLINE/DIGITAL SAFETY

FOR CHILDREN 7-12YRS

I am a Responsible Digital Citizen![1]

Useful terms to understand use of computers and computer networks

- Cyber

  Relating to the use of computers, network of computers (the internet) and information technology.

- Information and Communication Technology

  Relating to a system of sending, storing and receiving information.

- Cyber safety

  The safe and responsible use of information and communication technology. It is about keeping information safe and secure, being responsible with information, being respectful of other people online

- Digital citizen

  Someone who uses computers and computer networks. Digital citizens need to follow norms of appropriate and responsible use of technology.

- Digital Divide

  People across regions, genders, age groups and so on have different kinds and levels of access to computers and information technology. The digital divide talks of this imbalance, its effects and how to bridge gaps.

While on the internet, we come across:

- Search engines

  Search engines allow people to search for any kind of content on the World Wide Web (WWW). By entering keywords, users can find information in the form of websites, images, videos or other forms of digital data.

- Gaming

  Interactive games played through a mobile phone or computer or other electronic devices. The internet allows for multiple players in a game, making it a group activity too.

[1] These rules are aimed at mostly younger children, at oldest pre-teens. Appropriate “rules” for online use vary by age, maturity of the child and family values/principles. (update June 2013)

- Video Sharing

  A feature that allows users to upload, view and share videos across the web. Users have access to information and entertainment, making it very popular across age groups.

- Text messaging

  Short text messages sent using mobile phones and wireless handheld devices.

- Social networking

  Social networking sites allow users to set up profiles of themselves and connect with others in a virtual community. It allows young users to share text messages, photos, videos, memes and so on with like-minded people, and to keep in constant touch with friends. Most social networking sites require users to be above 18 years of age in order for their safety.

MY SAFETY, MY STEPS

I have a right to be safe and also a responsibility towards it!

1. My time and space

My parents and I will, together, decide upon the time of the day and the amount of time I spend online. We will also decide what sites and areas I can explore while online. I will not access other areas or break these set rules, making sure I get the best out of the online experience, and not put myself in danger or at risk of online abuse.

2. My personal information

I will safeguard my personal information such as my last name, my address, telephone number, name of my school or address, similar information of my siblings and parents' work address/telephone number I will not share it online or offline with anyone without my parents' permission.

3. Seeking help

If I come across anything on the internet that makes me feel uncomfortable, I can and will immediately tell my parents about it so that they can help me.

4. Online friends

I will never agree to meet in person someone I 'meet' or 'talk to' online without first checking with my parents. If my parents agree to the meeting, I will first make sure that it is in a public place and will take a parent along. Sometimes, people we meet online may be pretending to be someone they are not and I can get into trouble or danger. I will not go to meet them with friends or brothers/sisters as I can still get into risk situation.

5. Sharing pictures

I will always discuss with my parents about what I can post/share online, especially pictures of myself or of friends and others. I will not post pictures that are inappropriate.

6. Bullying on the internet

I do not have to and will not respond to any messages that are mean, make me feel uncomfortable, are threatening or put pressure on me to do something that I know is wrong. It is not my fault if I get a message like that and if I do receive anything of that sort, I will tell my parents right away.

7. Safe downloading

I will ask my parents before downloading anything, installing software or doing anything that could harm our computer or mobile device, or put my and that of my family's privacy and safety at risk.

8. **Keeping passwords secure**

I will not give out my passwords to anyone (even my best friends) other than my parents. If I'm using a public computer as in a cyber center or cyber cafe, or even in school I will ensure that I logout of all my accounts before I leave the computer.

9. **Responsible user**

While making use of the information and entertainment I have access to on the internet, I will be a responsible online-citizen. I will never do anything that hurts anyone, including my friends, peers, family or puts them in danger or is against the law.

10. **Helping my parents**

I will help my parents understand how to have fun and learn things online and teach them things about the Internet, computers and other technology, while also ensuring our safety!

Common references

For definitions:

https://www.techopedia.com/definition/12708/search-engine-world-wide-web - Authored by Techopedia staff
https://www.storypark.com/child-safety/ - Storypark

http://www.digitalcitizenship.net/

For the steps:

http://www.safekids.com/kidsrules.htm.

https://protectkidsonline.ca/app/en/ - By the Canadian Centre for Child Protection

UNICEF report Child Online Protection in India

ONLINE/DIGITAL SAFETY

FOR TEENAGERS

I am a Responsible Digital Citizen!

Useful terms to better understand the online experience

- Cyber

  Relating to the culture and use of computers, network of computers (the internet), information technology, and virtual reality.

- Information and Communication Technology

  Refers to technologies that provide access to information through telecommunications. This includes the Internet, wireless networks, cell phones, and other communication mediums in a system of receiving, sending and storing information.

- Cyber safety

  The safe and responsible use of information and communication technology. It is about keeping information safe and secure, being responsible with information, and being respectful of other people online.

- Digital citizen

  Someone who uses information and communication technology to engage with others in society. Digital citizenship suggests that there exist norms of appropriate and responsible use of technology.

- Digital Divide

  People across regions, genders, age groups and other differentiating factors have different kinds and levels of access to information technology. The digital divide talks of this unbalanced access, its effects and how to bridge gaps.

While on the internet, we come across:

- Search engines

  Search engines allow people to search for any kind of content on the World Wide Web (WWW). By entering keywords, users can find information in the form of websites, images, videos or other forms of digital data.

- Gaming

  Interactive games played through a mobile phone or computer or other electronic devices. The internet allows for multiple players in a game, making it a group activity too.

- Video Sharing

A feature that allows users to upload, view and share videos across the web. Users have access to information and entertainment, making it very popular across age groups.

- Text messaging

  Short text messages sent using mobile phones and wireless handheld devices.

- Social networking

  Social networking sites and applications allow users to set up their custom profiles and connect with others in a virtual community. It allows young users to share text messages, photos, videos, memes and so on with like-minded people, and to keep in constant touch with friends. Many social networking sites require users to be above 18 years of age in order for their safety.

- Applications

  Computer programs that run on smartphones, tablet computers and other mobile devices. Each program has a specific "application" or utility for the user, such as word processing, email, photography, gaming, and social networking and so on.

MY SAFETY, MY STEPS

I have a right to be safe and also a responsibility towards it!

1. My time and space

My parents and I will decide upon how much time I can spend online in a day and in what ways they can monitor my activities for my own safety while on the internet. This may include having them create an age appropriate account for me, and keeping track of the settings on the devices I use.

2. My personal information

The internet is a public space. I will always safeguard my personal information such as my last name, my address, telephone number, name of my school or address, similar information of my siblings and parents' work address/telephone numbers. Without consulting my parents, I will not give out personal information to anyone online or offline or share it on any forum even when asked to.

3. Seeking help

If I come across anything on the internet that makes me feel uncomfortable, I can and will immediately tell my parents or safe adults (who I trust) in school/college about it so that they can suggest how I deal with the situation. A little help is always welcome to understand how to navigate the internet and get the best out of it. Seeking help is not something to be shy or ashamed about. I will seek help rather than be in trouble!

4. Online friends

I will never agree to meet in person someone I “meet” or talk to online without first checking with my parents and verifying the identity of the person. If my parents agree to the meeting, I will be sure that it is in a public place. People we meet online may not be who they claim to be and may want to misuse the situation by making demands on me. I will not risk my safety. I will also not go to meet them with friends or brothers/sisters as we can still get into risk situation.

5. Privacy settings

I will always be sure to limit who can see text posts, pictures and videos I post online using the privacy settings on all apps. Most apps are by default set to “public” and are open to everyone’s access. I will approach my parents or safe adults in school to understand the different options on the settings.

6. Sharing pictures and videos

I do not have to and will not share my pictures or videos when I’m threatened by someone to do so or when conversations are turned sexual without my consent. I will remember that after posting pictures and videos on the internet, I no longer have full control over them and how they are used even if apps sometimes say they are temporarily shared. Likewise, I will also not share picture or videos of others when there is a possibility of misuse or abuse and can put them in a risk situation.

7. Bullying on the internet

I do not have to and will not respond to any harassing messages or ones that make me uncomfortable in any way. These are unsolicited and it is not my fault that I receive them. If I do receive anything of the sort, I will keep a record of it and tell my parents/safe adults right away. I can also block those persons who harass me or repeatedly send me unwanted messages.

8. Safe downloading

I will download applications from official stores and when I’m sure that anything I download will not harm our computer with any malware or jeopardize my family’s privacy or put us at risk. On a public computer, I will make sure I download only when necessary and keep personal downloads limited to our personal devices.

9. Keeping passwords secure

I will not give out my passwords to anyone, even my close friends. If I’m using a public computer, I will ensure that I logout of all my accounts before I leave the terminal.

10. Responsible user

While making use of the information and entertainment I have access to on the internet, I will be a responsible digital-citizen. I will treat others well, respect them and never do anything that hurts anyone, including my friends, peers, family or puts them in danger or is against the law.

11. Helping my parents

I will help my parents understand how to have fun and learn things online and teach about the internet, computers and other technology I have the opportunity to learn about, while also ensuring our safety.

ONLINE/DIGITAL SAFETY

FOR SCHOOL TEACHERS

Towards positive digital citizenship

Useful terminologies to better understand yours and your child's online experiences

- Cyber

  Relating to the culture and use of computers, internet, information technology, and virtual reality.

- Information and Communication Technology

  Technologies that provide access to information through telecommunications. This includes the Internet, wireless networks, cell phones, and other communication mediums in a system that is concerned with receiving, sending and storing information.

- Cyber safety

  The discourse of safe and responsible use of information and communication technology. It concerns keeping information secure, being responsible with available information, and being respectful of other people online. There is an urgent need to take steps towards children's safety online, to understand that possibilities of online sexual coercion and extortion of children (OSCEC) exist and to respond to situations effectively.

- Digital citizen

  Someone who uses information and communication technology to engage with society, culture, politics. Digital citizenship suggests that certain norms operate in the digital world as well and call for appropriate and responsible use of technology.

- Digital Divide

  Refers to the differential access to information technology among people across regions, genders, age groups and other differentiating factors. It also talks of the effects of the unbalanced access and how to address gaps.

Children's interests online

- Search Engines

  Search engines allow people to search for any kind of content on the World Wide Web (WWW). By entering keywords, users are shown results with links to information in the form of websites, images, videos or other forms of digital data. A great opportunity to learn about things.

- Gaming

While younger children are newly introduced to the world of gaming, older ones may have found their favourite genres. Interactive elements make online gaming very engaging and having multiple players makes it a popular group activity, exposing children to other users. These can be downloaded as apps or can be played directly on networking sites.

- Text messaging

  Short text messages sent using mobile phones and wireless handheld devices. Most text messaging now takes place on different social networking applications with varying chat features and different privacy policies.

- Video sharing

  A feature that allows users to upload, view and share videos across the web. This mode of access to information and entertainment makes it very popular across age groups.

- Social networking

  Social networking sites and applications allow users to set up their custom profiles and connect with others in a virtual community. They allow all users to share text messages, photos, videos, memes and so on with like-minded people, and to keep in constant touch with friends. Many social networking sites require users to be above 18 years of age in order for their safety. Many social networking sites require users to be above 18 years of age in order for their safety.

- Applications

  Computer programs that can be installed and run on smartphones, tablet computers and other mobile devices. Each program has a specific “application” or utility for the user, such as word processing, email, photography, gaming, and social networking and so on.

STEPS TOWARDS CYBER SAFETY FOR OUR CHILDREN

1. Moderation and accountability

We will always make sure that computer usage by children in school will be monitored by the Teaching staff. Children’s online activity will be moderated through age appropriate filters. We will frame rules around what content can be accessed from school and explain to the children why it is important for their own safety online.

2. Orientation to cyber use

We will organize age appropriate orientation to all children of the school on responsible Digital Citizenship and cyber/online safety, ensuring that the children and the school authorities are on the same page on the rules and requirements of cyber use.

3. Securing personal information

The internet is a public space and children need to understand not to share personal information on any online forum without consulting adults they trust, such as parents and members among the teaching staff. We will ensure that we communicate the importance of this to children. Personal information will include things like last name, home address, telephone number, name and address of the school, similar information about siblings, parents' work address/ phone numbers.

4. Social network accounts

We will mandate that children not have access to social networking through school computers or personal mobiles during school hours, unless in specific cases or requirements with the permission of the management and knowledge of parents/guardians.

5. Editing privacy settings

The default settings on many applications are on "public" allowing any other user to access the shared data. While a few apps allow parental control features, others may not. We will make sure to remind parents to review content of apps for age appropriateness and help children understand how to use the privacy settings to secure their data.

6. Consent and sharing

Orientation will include conversations with children on consent and how there may be instances when they are threatened on the internet to share pictures or videos of themselves or others. We will regularly discuss what is appropriate for sharing and about never sharing things that can put them at risk or harm them, their family and others.

7. Building trust

We will always keep communication channels open with children and listen to them so that they can approach us for help if they come across anything on the internet that makes them uncomfortable. Discussing with them about appropriate and responsible use goes a long way, apart from a sense of security derived from setting parental controls across platforms and apps.

8. Reporting cyber bullying, harassment

We will talk to children about possibilities of bullying, harassment, stalking and abuse online by users. We will help them understand that they may come across predatory behaviour on the internet and that it is not their fault if they receive harassing messages, and that sending such messages is a crime. We will teach them to keep a record in case they receive such messages or images and to approach us or their parents in order to report the crime. We will ensure that we do not at any point of time make them feel guilty or ashamed of what has happened.

9. Safe downloading

We will make sure to teach young users about the risks of and how to avoid downloading malware that can harm the school computer or their personal computers at home, or that compromises their and their family's privacy.

10. Responsible, productive use

We will do our best to follow and convey to children the norms of good digital citizenship while making use of the information and entertainment that we have access to. We will talk to them about the laws regarding cyber culture in the country and how to report abuse. We will help them understand the need to treat others well and to never do anything online that hurts them or anyone else, or is against the law.

11. Learning from our young ones

We can and will be happy to learn from young users about the internet and its various strengths and possibilities. Together, we will make learning fun for all. If and when children are victims or perpetrators of cyber abuse, we will approach the situation with caution, understanding that they need care, support and guidance.

12. Oathfor Child Protection

We will ensure that parents/guardians and students have read and signed the child protection for our safe school that also includes steps to be taken for Responsible digital citizenship and cyber/online safety.

ONLINE/DIGITAL SAFETY

FOR PARENTS

Towards positive digital citizenship

Useful terminologies to better understand yours and your child's online experiences

- Cyber

  Relating to the culture and use of computers, internet, information technology, and virtual reality.

- Information and Communication Technology

  Technologies that provide access to information through telecommunications. This includes the Internet, wireless networks, cell phones, and other communication mediums in a system that is concerned with receiving, sending and storing information.

- Cyber safety

  The discourse of safe and responsible use of information and communication technology. It concerns keeping information secure, being responsible with available information, and being respectful of other people online. There is an urgent need to take steps towards children's safety online, to understand that possibilities of online sexual coercion and extortion of children (OSCEC) exist and to respond to situations effectively.

- Digital citizen

  Someone who uses information and communication technology to engage with society, culture, politics. Digital citizenship suggests that certain norms operate in the digital world as well and call for appropriate and responsible use of technology.

- Digital Divide

  Refers to the differential access to information technology among people across regions, genders, age groups and other differentiating factors. It also talks of the effects of the unbalanced access and how to address gaps.

Children's interests online

- Search Engines

  Search engines allow people to search for any kind of content on the World Wide Web (WWW). By entering keywords, users are shown results with links to information in the form of websites, images, videos or other forms of digital data. A great opportunity to learn about things.

- Gaming

While younger children are newly introduced to the world of gaming, older ones may have found their favourite genres. Interactive elements make online gaming very engaging and having multiple players makes it a popular group activity, exposing children to other users. These can be downloaded as apps or can be played directly on networking sites.

- Text messaging

  Short text messages sent using mobile phones and wireless handheld devices. Most text messaging now takes place on different social networking applications with varying chat features and different privacy policies.

- Video sharing

  A feature that allows users to upload, view and share videos across the web. This mode of access to information and entertainment makes it very popular across age groups.

- Social networking

  Social networking sites and applications allow users to set up their custom profiles and connect with others in a virtual community. They allow all users to share text messages, photos, videos, memes and so on with like-minded people, and to keep in constant touch with friends. Many social networking sites require users to be above 18 years of age in order for their safety.

- Applications

  Computer programs that can be installed and run on smartphones, tablet computers and other mobile devices. Each program has a specific “application” or utility for the user, such as word processing, email, photography, gaming, and social networking and so on.

STEPS TOWARDS CYBER SAFETY FOR OUR CHILDREN

1. **Balancing moderation and privacy**

It is important that parents and children together decide when and for how long each day children spend time online and follow these rules. We will make sure to work together to monitor the child’s activity online through steps like using age appropriate filters, while also keeping in mind their need for privacy as they grow up.

2. **Setting up accounts**

We can begin with creating accounts with appropriate privacy settings in place for young children. We will impress upon young and older children that passwords must not be shared with anyone other than parents, not even close friends and that it is easy to lose control over personal information if passwords are shared. We will remind them that they need to logout of all accounts while using public computers like in school or cyber centers.

3. **Securing personal information**

The internet is a public space and children need to understand not to share personal information on any online forum without consulting safe adults. We will ensure that we communicate the importance of this to our children. Personal information will include things like last name, home address, telephone number, name and address of the school, similar information about siblings, parents' work address/ phone numbers.

4. Editing privacy settings

The default settings on many applications are on "public" allowing any other user to access the shared data. While a few apps allow parental control features, others may not. We will make sure to review content of apps for age appropriateness and help children understand how to use the privacy settings to secure their data.

5. Consent and sharing

We will begin conversations with children on consent and how there may be instances when they are threatened on the internet to share pictures or videos of themselves or others. We will regularly talk about what is appropriate for sharing and about never sharing things that can put them at risk or harm them, their family and others.

6. Building trust

We will always keep communication channels open with children and listen to them so that they can always approach us for help or if they come across anything on the internet that makes them uncomfortable. Discussing with them about appropriate and responsible use goes a long way, apart from a sense of security derived from setting parental controls across platforms and apps.

7. Reporting cyber bullying, harassment

We will talk to children about possibilities of bullying, harassment, stalking and abuse online by users. We will help them understand that they may come across predatory behaviour on the internet and that it is not their fault if they receive harassing messages, and that sending such messages is a crime. We will teach them to keep a record in case they receive such messages or images and to approach us/safe adults in order to report the crime. We will ensure that we do not at any point of time make them feel guilty or ashamed of what has happened.

8. Safe downloading

It is important to understand what young children are interested in and download it for them, to avoid risks of inappropriate content being downloaded. We will make sure to teach young users about the risks of accidentally downloading malware that can harm the computer or put our privacy at risk. We will learn the different features of parental control on downloading on mobile devices.

9. Responsible, productive use

We will do our best to follow and convey to children the norms of good digital citizenship while making use of the information and entertainment that we have access to. We will talk to them about the laws regarding cyber culture in the country and how to report abuse. We will help them understand the need to treat others well and to never do anything online that hurts them or anyone else, or is against the law.

10. **Learning from our young ones**

We can and will be happy to learn from young users about the internet and its various strengths and possibilities. Together, we will make learning fun for all. If and when children are victims or perpetrators of cyber abuse, we will approach the situation with caution, understanding that they need care, support and guidance.

Towards positive digital citizenship

Useful terminologies to better understand yours and your child's online experiences

- Cyber

  Relating to the culture and use of computers, internet, information technology, and virtual reality.

- Information and Communication Technology

  Technologies that provide access to information through telecommunications. This includes the Internet, wireless networks, cell phones, and other communication mediums in a system that is concerned with receiving, sending and storing information.

- Cyber safety

  The discourse of safe and responsible use of information and communication technology. It concerns keeping information secure, being responsible with available information, and being respectful of other people online. There is an urgent need to take steps towards children's safety online, to understand that possibilities of online sexual coercion and extortion of children (OSCEC) exist and to respond to situations effectively.

- Digital citizen

  Someone who uses information and communication technology to engage with society, culture, politics. Digital citizenship suggests that certain norms operate in the digital world as well and call for appropriate and responsible use of technology.

- Digital Divide

  Refers to the differential access to information technology among people across regions, genders, age groups and other differentiating factors. It also talks of the effects of the unbalanced access and how to address gaps.

Children's interests online

- Search Engines

Search engines allow people to search for any kind of content on the World Wide Web (WWW). By entering keywords, users are shown results with links to information in the form of websites, images, videos or other forms of digital data. A great opportunity to learn about things.

- Gaming

  While younger children are newly introduced to the world of gaming, older ones may have found their favourite genres. Interactive elements make online gaming very engaging and having multiple players makes it a popular group activity, exposing children to other users. These can be downloaded as apps or can be played directly on networking sites.

- Text messaging

  Short text messages sent using mobile phones and wireless handheld devices. Most text messaging now takes place on different social networking applications with varying chat features and different privacy policies.

- Video sharing

  A feature that allows users to upload, view and share videos across the web. This mode of access to information and entertainment makes it very popular across age groups.

- Social networking

  Social networking sites and applications allow users to set up their custom profiles and connect with others in a virtual community. They allow all users to share text messages, photos, videos, memes and so on with like-minded people, and to keep in constant touch with friends. Many social networking sites require users to be above 18 years of age in order for their safety. Many social networking sites require users to be above 18 years of age in order for their safety.

- Applications

  Computer programs that can be installed and run on smartphones, tablet computers and other mobile devices. Each program has a specific “application” or utility for the user, such as word processing, email, photography, gaming, and social networking and so on.

STEPS TOWARDS CYBER SAFETY FOR OUR CHILDREN

1. **Moderation and accountability**

We will always make sure that computer usage by children in school will be monitored by the Teaching staff. Children’s online activity will be moderated through age appropriate filters. We will frame rules around what content can be accessed from school and explain to the children why it is important for their own safety online.

2. **Orientation to cyber use**

We will organize age appropriate orientation to all children of the school on responsible Digital Citizenship and cyber/online safety, ensuring that the children and the school authorities are on the same page on the rules and requirements of cyber use.

3. Securing personal information

The internet is a public space and children need to understand not to share personal information on any online forum without consulting adults they trust, such as parents and members among the teaching staff. We will ensure that we communicate the importance of this to children. Personal information will include things like last name, home address, telephone number, name and address of the school, similar information about siblings, parents' work address/ phone numbers.

4. Social network accounts

We will mandate that children not have access to social networking through school computers or personal mobiles during school hours, unless in specific cases or requirements with the permission of the management and knowledge of parents/guardians.

5. Editing privacy settings

The default settings on many applications are on "public" allowing any other user to access the shared data. While a few apps allow parental control features, others may not. We will make sure to remind parents to review content of apps for age appropriateness and help children understand how to use the privacy settings to secure their data.

6. Consent and sharing

Orientation will include conversations with children on consent and how there may be instances when they are threatened on the internet to share pictures or videos of themselves or others. We will regularly discuss what is appropriate for sharing and about never sharing things that can put them at risk or harm them, their family and others.

7. Building trust

We will always keep communication channels open with children and listen to them so that they can approach us for help if they come across anything on the internet that makes them uncomfortable. Discussing with them about appropriate and responsible use goes a long way, apart from a sense of security derived from setting parental controls across platforms and apps.

8. Reporting cyber bullying, harassment

We will talk to children about possibilities of bullying, harassment, stalking and abuse online by users. We will help them understand that they may come across predatory behaviour on the internet and that it is not their fault if they receive harassing messages, and that sending such messages is a crime. We will teach them to keep a record in case they receive such messages or images and to approach us or their parents in order to report the crime. We will ensure that we do not at any point of time make them feel guilty or ashamed of what has happened.

9. Safe downloading

We will make sure to teach young users about the risks of and how to avoid downloading malware that can harm the school computer or their personal computers at home, or that compromises their and their family's privacy.

10. Responsible, productive use

We will do our best to follow and convey to children the norms of good digital citizenship while making use of the information and entertainment that we have access to. We will talk to them about the laws regarding cyber culture in the country and how to report abuse. We will help them understand the need to treat others well and to never do anything online that hurts them or anyone else, or is against the law.

11. Learning from our young ones

We can and will be happy to learn from young users about the internet and its various strengths and possibilities. Together, we will make learning fun for all. If and when children are victims or perpetrators of cyber abuse, we will approach the situation with caution, understanding that they need care, support and guidance.

12. Oathfor Child Protection

We will ensure that parents/guardians and students have read and signed the child protection for our safe school that also includes steps to be taken for Responsible digital citizenship and cyber/online safety.