مدرسة دروف العالمية ذ م م
Dhruv Global School L L C

DHRUV GLOBAL SCHOOL

Cyber security Policy

2025-26

1. Purpose

This policy ensures a secure digital learning environment by promoting responsible online behavior, protecting personal information, and preventing cyber threats for both students and staff in the school premises.

2. Guidelines for Students

Safe Internet Usage:

A. **Use the internet strictly for learning.**

Example: When researching for a science project, students should use trusted educational sites like NASA Kids instead of random search results.

B. **Avoid accessing social media and gaming websites during school hours.**

Example: Platforms like TikTok and online multiplayer games should not be used on school devices.

C. **Parents and teachers should supervise online activities.**

Example: A parent can use parental controls to monitor screen time and block harmful c content.

Personal Information Protection: -

A. Never share personal details online.

Example: A student should not post their name, address, or school details when signing up for an online game or app.

B. Use strong passwords and keep them confidential.

Example: Instead of using “123456,” a student should create a unique password like “BlueSky#2025” and never share it with friends.

C. Report cyber bullying or online threats immediately.

Example: If a student receives inappropriate messages on a class forum, they should report it to their teacher.

Responsible Use of Devices: -

A. **Take care of school devices and avoid installing unauthorized apps.**

Example: A student should not download unknown apps on a school tablet as they may contain malware.

B. **Always log out after using shared devices to protect accounts**.

Example: After completing an assignment on a school computer, students must log out to prevent unauthorized access.

Cyber Ethics and Digital Citizenship

A. **Communicate respectfully online.**

Example: In a class group chat, students should use polite language just as they would in real conversations.

B. **Do not copy copyrighted content without permission.**

Example: When working on a history project, students must cite sources instead of copying text directly from Wikipedia.

C. **Avoid clicking on suspicious links or emails.**

Example: If a student receives an email claiming they won a prize they never entered for, they should delete it and inform an adult.

3. Guidelines for Teachers & Staff

Digital Security & Data Protection

A. Use strong passwords and enable multi-factor authentication.

Example: A teacher should use different passwords for email and school portals, and enable OTP verification for added security.

A. Keep student data secure and avoid sharing sensitive information externally.

Example: Student grades should be stored in encrypted files and not shared via personal emails.

B. **Update school devices regularly to prevent security risks.**

Example: The IT department should install security patches and antivirus updates on all school computers every month.

Responsible Use of Technology

A. **Use school-provided devices and platforms for work purposes only.**

Example: Teachers should not use school laptops for personal shopping or social media browsing.

B. **Monitor student online behavior and reinforce safe practices.**

Example: Teachers should educate students on responsible internet use, such as avoiding sharing personal details online.

C. **Avoid downloading unauthorized software without IT approval.**

Example: Before installing any new educational app, teachers should get approval from the IT department.

Cyber Ethics & Communication

A. **Maintain professionalism in all online interactions**.

Example: All emails sent to students and parents should be formal and aligned with school guidelines.

B. **Be cautious about phishing attempts and suspicious emails.**

Example: If a teacher receives an unexpected email asking for login credentials, they should report it to IT instead of clicking on the link.

C. **Educate students on responsible internet usage through awareness programs**.

Example: Organizing a “Cyber Awareness Week” where students engage in interactive cyber security workshops.

4. Reporting & Incident Management

A. Report any cybersecurity incidents or suspicious activity to IT.

Example: If a staff member notices unauthorized access to student records, they must notify the school administration immediately.

B. Follow school protocols for managing cyber threats.

Example: In case of a phishing attack, affected accounts should be reset, and a cybersecurity briefing should be conducted to prevent future incidents.

By implementing this policy, we ensure a safe and ethical digital learning environment for students and staff.

Ministry of Interior and the National Programmer for Happiness and Wellbeing launched the ‘Child Digital Safety’ initiative in March 2018, in a joint effort to raise awareness among children and school students about online threats and challenges, and promote a safe and constructive use of the internet

ITU’s Child Online Protection (COP) Guidelines

ITU launched the 2020 Child Online Protection (COP) Guidelines to ensure that the rights of children are being respected when they are online. The guidelines are the product of the collaborative effort of 80 experts from different sectors including governments, international organisations, NGOs, academia and the private sector.

Four sub-initiatives to enhance digital safety of children

This initiative consists of four main sub-initiatives. They are:

- Interactive Children’s Camp, where children between 5 and 18 years can learn how to use the internet and social media safely
- Digital Wellbeing Portal, which provides tools and information to help parents face the challenges of the digital world
- training workshops, where parents and teachers can be trained to address digital challenges and threats and
- A support platform to answer urgent queries from parents regarding digital safety.

Protection of children's data online

- **Article 29 of Federal Law No. 3 of 2016 Concerning Child Rights, also known as Wadeema's Law (PDF, 250 KB), states: The telecommunications companies and internet service providers shall notify the competent authorities or the concerned entities of any child pornography materials being circulated through the social media sites and on the Internet and shall provide necessary information and data on the persons, entities or sites that circulate such material or intend to mislead the children.**
- **The Sannif initiative was launched to enable parents to learn about eGames and assess their impact on their children.**

Game and App for children

To encourage children to learn how to stay safe online, ITU and partners are offering two innovative complementary products, allowing children and youth to learn through play:

- Sango's Adventures: discover online safety for younger children
- Ask Me, your online safety friend for teens. The interactive and playful tools are
- adapted to different age groups, making learning even more fun.

Tips for PARENTS:

- Have a discussion with your children
- try and **do some online activities with them.**
- **Consider age** of digital consent.
- Educate children on the **dangers of meeting up** with a stranger.
- **Identify the technology, devices** and services across your family / household.
- Control **use of credit cards** and other payment mechanisms.
- Help your children understand and **manage their personal information.**
- Consider whether **filtering and blocking or monitoring programmers** can help and support your family.
- Know **how to report problem.**
- Ensure children and young people understand what it means to **post photographs**

- on the Internet.
- Agree expectations as a **family about using the internet** and personal devices.
- Be aware that **advertising can be inappropriate** or misleading.
- Be aware of the **online and mobile services** used by your children.
- Create a **culture of support** in the home so that children and young people feel able to seek support.

Tips for Educators

- Ensure that all devices are **secure and password protected**.
- Raise awareness of the importance of **digital footprint and online reputation**.
- Install **anti-virus** software and firewalls.
- Recognize the importance of **professional online communication** with pupils, parents and other stakeholders.
- Ensure that there is a **policy which details** how technology can be used.
- Understand the **risks and benefits** that pupils can be exposed to when they go online.
- Ensure that internet feed provided by the school is **filtered and monitored.**
- **Child Online Protection, an ITU initiatives.**