DPS GROUP OF INSTITUTIONS

Policies & Procedure of
Information Communication Technology (ICT)

(Essentials of ICT Policy)

Document Owner

Director of IT
DPS Group of Institutions
P.O. Box 14868, Doha, Qatar

Change History

Issue No.	Date	Description of Change
1.0	April 2024	Preparation and Major update to IT policies.
1.1	January 2026	Revision in iPad Policies and Charging station Policies
1.1	April 2026	Discontinued BYOD program

Document Version

Version Number:	1.1
Effective Date:	April 2026
Endorsed by IT Director on:	April 2026

Distribution List

This document is controlled by the IT Director and is available to others upon approval.

S/N	Position	Remarks
1	IT Director	Controlled
2	Institution / Heads of DPS Group of Institutions	Controlled
3	Heads of all key functions, but not limited to, IT, Facility, Transport, Security, Finance	Uncontrolled
4	End Users in DPS Group	Uncontrolled

Contents

DPS Group IT Services Core Values

The Information Technology department (IT) is recognized as the provider of IT services at DPS Group. The **Teaching Community** benefits from state-of-the-art classroom technologies, learning management systems, other IT resources, and network coverage that extends to all corners of the campus of all the institutions of DPS Group.

For **the Admin Staff**, the technological solutions provided by the IT department are the best solutions as per international standards.

The IT policies included in this document are in line with the following core values:

- **Collaboration:** both within IT and with those we serve—Stakeholders, as it helps us understand and support the technology needs of the entire DPS Group community.
- **Continuous Improvement:** We strive for operational excellence through the on-going development of the staff and the DPS Group as a whole.
- **Innovation:** We encourage creative and critical thinking in the development of technology services and solutions.
- **People:** We listen to, respect and care for students, faculty, staff, and one another, both professionally and personally.
- **Service:** We strive to provide excellent service by being consistent, agile, available, reliable and accessible to all.
- **Transparency:** We leverage open communications and thoughtful business processes to be accountable in our interactions and our work.

1. IT Resource Usage Policy

1.1 Policy Description

This policy outlines the acceptable use of IT resources at DPS Group of Institutions to ensure security, productivity, and alignment with our educational mission.

1.2 Purpose

To provide clear guidelines for staff and students on how to responsibly use IT resources, including devices, networks, and software.

1.3 Scope

This policy applies to all users of DPS Group IT resources.

1.4 Policies and Procedures

a. DPS Group provides its users with information technology resources to support academic, educational, administrative, public service, and research activities.
b. Users are responsible for adhering to the highest standards of ethical, considerate and proper use of such resources to serve these purposes, regardless of their affiliation with the University.
c. All users of DPS Group are required to adhere to the policy sections below.

1.4.1 General Terms

1.4.1.1 Acceptable Use

The use of DPS Group IT Resources should be for the purposes that are consistent with the educational mission, policies and legal requirements of the DPS Group of Institutions, including license agreements and terms of service of the Institutions, and not for commercial purposes.
Users may use only the DPS Group IT Resources for which they have authorization and for the purpose of conducting DPS Group business activities.

1.4.1.2 Prohibited Use

Users are not permitted to access DPS Group IT Resources for any unauthorized purposes which are not related to DPS Group business activities. The utilization of DPS Group IT Resources should align with the educational mission, policies, and legal requirements of the DPS Group of Institutions. This includes adhering to license agreements, terms of service, and refraining from commercial use.

The following activities are strictly prohibited:

- **Unauthorized Access**: Attempting to access systems or data without proper authorization.
- **Malware and Hacking**: Introducing malicious software or engaging in hacking activities.
- **Personal Use**: Excessive personal use of organizational devices or networks, including but not limited to social media, streaming, and gaming.
- **Inappropriate Content**: Accessing, storing, or distributing illegal, offensive, or inappropriate content.
- **Bypassing Security**: Circumventing security measures or policies, including disabling firewalls and antivirus software.
- **Unauthorized Software**: Installing or using unapproved software or applications.
- **Data Sharing**: Sharing sensitive organizational data with unauthorized individuals or entities.

Consequences:

Violations of the IT resources policy in DPS Group may result in various consequences based on the severity of the infraction. The following outlines potential repercussions:

Disciplinary Actions

- **Verbal Warning**: For minor infractions, a verbal warning may be given by a teacher or administrator.
- **Written Warning**: Repeated or more serious violations may result in a formal written warning, which will be documented.
- **Loss of Privileges**: Students/Staffs may lose access to school computers, networks, or other technology resources for a specified period.
- **Detention or Suspension**: Serious violations, such as accessing inappropriate content or engaging in cyberbullying, may lead to detention or suspension from school.
- **Expulsion**: Severe infractions, especially those involving illegal activities or threats to safety, may result in expulsion from the school.
- **Reporting to Authorities**: In cases involving illegal activities (e.g., hacking, distribution of illegal content), the school may notify law enforcement authorities.

Exceptions:

While the IT resources policy in DPS Group outlines prohibited uses, there are certain circumstances under which exceptions may be granted by the Management/Principal. These exceptions ensure that technology can be used effectively while maintaining security and appropriate usage standards.

1. Educational Purposes

- **Classroom Activities**: Students may access specific websites or applications that are necessary for class assignments, projects, or research, as directed by teachers.
- **Educational Programs**: Participation in approved educational programs or online courses may warrant temporary access to restricted resources.

2. Special Projects

- **Approved Projects**: Students working on special projects, presentations, or extracurricular activities may receive temporary access to additional resources with prior approval from a teacher or administrator.

3. School-Sponsored Events

- **Events and Competitions**: During school-sponsored events, such as science fairs or technology competitions, exceptions may be made to allow students to use specific tools or platforms that support their projects.

4. Emergency Situations

- **Crisis Management**: In the event of an emergency, students may be granted access to additional resources to ensure their safety or to support communication efforts.

5. Parental or Guardian Requests

- **Supervised Use**: Parents or guardians may request specific exceptions for their child under supervision, with prior notification to school staff.

Approval Process:

All exceptions must be approved in advance by the Principal/Management and evidence of approval must be submitted to the IT Department. Requests for exceptions should be submitted in writing, providing a rationale and timeframe for the exception.

1.4.1.3 Accountability

Users of DPS Group IT Resources are individually responsible and accountable for the appropriate use of the resources assigned to them or which they are authorized to access.

1.4.2 Use of Computing Devices

Users of DPS Group-owned and DPS Group-managed computing devices are expected to acknowledge and comply with the following guidelines:

1. **Ownership and Care**: All computing devices provided by DPS Group are the property of the institution. Users must handle these devices responsibly to prevent physical damage, failure, or misuse.
2. **Device Configuration**: The IT Department is responsible for managing the configuration of all DPS Group-owned and managed devices. IT has final authority on the installation and configuration of software or applications on these devices.
3. **Administrative Privileges**: Users do not have administrative privileges on DPS Group-owned or managed devices and should not expect such access.
4. **Repairs and Formatting**: Users are prohibited from attempting to format, repair, or make unauthorized modifications to any DPS Group-managed computing device.

Prohibited Uses

Users shall not use DPS Group computing devices to:

8. **Unauthorized Access**: Access data, computers, accounts, or networks without authorization or in violation of laws or policies.
9. **Offensive Content**: Distribute, share, or store offensive, abusive, or harmful material.
10. **Malicious Software**: Install, distribute, or knowingly execute malware or other malicious software that could damage systems, result in data loss, or disrupt network operations.
11. **Circumvent Security**: Attempt to bypass established security measures to access confidential or restricted information.
12. **Unlicensed Software**: Install or distribute unlicensed software or software in violation of copyright laws.
13. **Fraudulent Activities**: Create, transmit, or participate in activities such as pranks, hacking attempts, chain letters, misinformation, or other unlawful actions.
14. **Legal Violations**: Violate local laws, Qatari regulations, international laws, or any contractual obligations.
15. **Unauthorized Modifications**: Attempt to format, repair, or modify DPS Group-owned devices without prior approval from the IT Department.

1.4.3 Use of Staff Laptop

This policy establishes guidelines and responsibilities for the use of school-issued laptops by staff. All staff members are expected to adhere to the following:

1.4.3.1 Laptop Usage Guidelines

1. **Laptop Acceptance**
   Staff must sign the Laptop Acceptance Form prior to receiving a school-issued laptop. Before acceptance, they are required to carefully inspect the device for any existing damage (e.g., cracks, dents, scratches). Once accepted, claims regarding pre-existing damage will not be entertained.
2. **Provision of Laptops**
   School-issued laptops are provided to support staff in fulfilling their duties and responsibilities. However, collecting a school-issued laptop is not mandatory. Staff may use personal laptops for work purposes upon receiving approval from their Line Manager and the Principal. Personal devices must be compatible with the school's network and the required software, with support available from the IT Department.
3. **Purpose of Use**
   School-issued laptops are intended strictly for educational, administrative, and official communication purposes. Devices are pre-installed with licensed software and operating systems approved by the school.
4. **Unlicensed Software**
   Staff are solely responsible for any unlicensed software they install and for any legal, technical, or financial consequences resulting from such installations.
5. **Personal Use**
   Limited personal use is permitted, provided it does not interfere with professional responsibilities and adheres to this policy.
6. **Ownership**
   All laptops and related accessories remain the property of the school. Devices are assigned for use during a period determined by school administration.

7. **Modifications and Configurations**
   Staff must not install or modify any software, hardware, or system/network configurations without prior written approval from the IT Department.
8. **Issuance of Accessories**
   Upon issuing a laptop, the following accessories will be provided:
   - Laptop charger and charging cable
   - Laptop bag

   Additional accessories such as a mouse or external keyboard are not provided and may be purchased individually by staff.
   Note: Accessories like HDMI cables, stylus pens (for interactive panels), and RFID cards (for printers) may be issued based on specific needs. Any loss, theft, or damage to such equipment will be subject to the policies outlined in this agreement.
9. **Care and Security**
   Staff must take reasonable precautions to prevent damage, theft, or misuse of laptops. Devices should not be left unattended in unsecured or high-risk areas.
10. **Protection and Screen Care**
    Staff are responsible for general care of the laptop. Any functional issues or accidental damage must be reported to the IT Department immediately along with an incident report.

    Screen Care: Screens are sensitive and should not be subjected to pressure or rough handling. Clean the screen only with soft, dry or anti-static cloth. Do not use liquid or chemical cleaners.

    General Care:
    - Devices must remain free of any writing, drawing, stickers, or labels except those applied by the school.
    - Use laptops on flat, stable surfaces to ensure ventilation and prevent overheating.
    - Avoid placing food or drinks near the laptop.
    - Do not expose laptops to extreme temperatures or sudden temperature changes.
11. **Theft Reporting**
    In the event of theft, staff must immediately report the incident to the school administration and IT Department. If the device is not recovered, staff may be held financially responsible for the loss.
12. **Damage and Repair Costs**
    Staff will be held financially accountable for any damage resulting from negligence or misuse (e.g., cracks, dents, liquid damage). Repair or replacement costs will be based on vendor quotations and communicated prior to any salary deductions.
13. **External Damages**
    Staff are responsible for damages occurring outside school premises or resulting from external factors such as malware, accidental drops, or mishandling.
14. **Normal Wear and Tear**
    Reasonable wear and tear will not be penalized. However, damages due to carelessness or mishandling will be addressed as per this policy.
15. **File Management and Data Backup**
    Staff are responsible for managing their data and ensuring regular backups to the school's official cloud storage (e.g., OneDrive). In the event of data loss, staff must attempt recovery and may consult the IT Department for assistance.
16. **Acceptable Use & Legal Compliance**
    Laptops must be used in accordance with this policy, all applicable license agreements, and Qatari local laws. Use or possession of unauthorized software or hacking tools is strictly prohibited and may result in disciplinary or legal action.
17. **Privacy and Data Monitoring**
    Staff are advised not to store personal data such as photos, videos, and documents on school-issued laptops. The school reserves the right to inspect any data stored on its devices for maintenance, audits, or legal investigations.
18. **Periodic IT Inspections**
    Laptops must be periodically submitted to the IT Department for inspection and updates. This ensures all devices are compliant with security protocols and function effectively.

1.4.4 Use of iPad/Android Tablets: Grade 1 – 5 (For Monarch International School)

To enhance the learning process of students, as part of school curriculum activities, students are advised to use tablets on the school campus for digital assessments (Concept Recap), research for project work, ICT, and other interactive educational activities only.

1.4.4.1 iPad/Android Tablets Policy

As part of our commitment to providing a dynamic and engaging learning environment, tablets are integrated into the educational experience for students in Grades 1–5. This policy outlines the proper use, care, and maintenance of tablets to ensure they are utilized effectively for academic purposes. Guidelines are designed to protect both devices and students, while ensuring that technology enhances learning in a safe, secure, and responsible manner.

1. Acceptable Use

- Tablets must be used exclusively for school-related activities, including:
  - Digital assessments (Concept Recap)
  - Research for projects and assignments
  - Interactive educational activities
  - Accessing school-approved apps (e.g., Microsoft OneDrive, Office Mail, Teams, Forms)
- Students must follow teacher instructions regarding tablet usage during class.

2. Prohibited Use

- Installing unauthorized apps or software, including VPNs
- Accessing inappropriate or non-educational content
- Using tablets for personal entertainment (e.g., games, social media, streaming)
- Sharing tablets without teacher permission
- Attempting to bypass school security or network restrictions
- Using LTE or cellular-enabled tablets (SIM-supported models are strictly prohibited)

1.4.4.2 General Terms and Conditions

In order to ensure the safe and effective use of iPad/Android tablets for educational purposes, the following general guidelines outline the responsibilities and expectations for students, parents, and staff.

1.4.4.2.1 General Guidelines

1. **Educational Use Only:** Tablets must be used solely for learning purposes.
2. **Device Specifications**:
   - iPad: Generation 8th or later, iPadOS 14 or newer
   - Android 14 or newer, with full Google Play Store access (devices without official Play Store support, such as certain Huawei models, are not allowed).
   - Screen Size: 10–12 inches only
   - RAM: Minimum 4 GB
   - Storage: Minimum 64 GB
   - Connectivity: Wi-Fi only (tablets with SIM/cellular are strictly not allowed)
   - Approved Android Brands: Google Pixel Tablet, Samsung Galaxy Tab series, Lenovo Tab series (only models with official Google Play Store support), Xiaomi/Redmi tablets (only stock MIUI with Google Play Store), Realme Pad (stock Android with Google Play Store support)
   - Excluded / Not Allowed:
     - Any Huawei tablets or other brands without full Google Play Store access
     - Any obscure, unbranded, or imported tablets
3. **Charging Accessories:**
   - Parents must submit the tablet along with the charging cable. One end of the cable must be USB-A (male, standard USB), and the other end must be compatible with the tablet (Type-C, Lightning, Micro-USB, etc.).
   - Cables that do not support USB-A on one side will not be accepted.

4. **Parental Responsibility:**
   - Parents must purchase tablets that meet school specifications.
   - Tablets, along with the charging cable, must be submitted to the Homeroom Teacher (HRT) without any user account logged in and without any parental control enabled.
   - School-approved apps (details will be shared by the school) must be installed on the tablet before submission.
   - Once the apps are installed, parents must log out of all Google or Apple accounts on the device.
5. **Protection:** Tablets must have a sturdy, slim back cover and a tempered glass screen protector.
6. **Storage & Charging:**
   - Tablets remain in school throughout the academic year.
   - Class teachers will store and charge tablets in designated charging stations.
7. **Reporting Issues:** Any damage, malfunction, or loss must be reported immediately to the class teacher or IT department.
8. **Self-Declaration Form:** The "Self-Declaration Form" provided by the Homeroom Teacher (HRT) at the time of submitting the tablet and charging cable must be carefully read, completed, and signed by the parents.

1.4.4.2.2 Care and Maintenance

1. **Physical Care**
   - Use soft, dry cloth to clean the screen (no liquid/chemical cleaners).
   - Avoid extreme temperatures, heavy objects, and liquids near the iPad.
   - Store securely in charging stations when not in use.
2. **Damage and Repairs**
   - Parents bear repair costs for damages due to negligence.
   - Warranty does not cover misuse (e.g., liquid spills, cracked screens).
   - Report damage to the class teacher/IT department.
   - Repairs will be coordinated with authorized service centers.
3. **Theft or Loss**
   - Report theft/loss immediately to the class teacher, IT department, and school security department.

1.4.4.2.3 General Use

- Tablets must be used at school whenever required. Students are responsible for bringing their tablet to all classes as directed by the teacher, unless specifically instructed otherwise.
- Charging stations with locker facilities are installed in classrooms.
- Grades may be impacted if students come to class without a charged tablet.

Sound, Music, and Video

- Sound must be always muted unless permission is obtained from the teacher for instructional purposes.
- Students are not allowed to use the tablets for personal entertainment while on the school network or in public at any time. Personal entertainment includes video, music, and games that are not part of the class curriculum.

1.4.4.2.4 File Management

- Students are responsible for managing their data and ensuring regular backups.
- Files may be saved on the tablets, but students are encouraged to use cloud storage (e.g., OneDrive) or email important documents to themselves as a precaution.
- Limited storage is available on the tablets. If the device needs to be reset, files may be lost, and it is the student's responsibility to prevent data loss.
- Tablet malfunctions or accidental deletions are not valid excuses for missing coursework.
- The school does not guarantee uninterrupted network access. In case of network downtime, the school is not responsible for any lost or missing data

1.4.4.2.5 Apps and Settings

1. **School-Recommended Apps:** Only approved apps should be installed.

2. **Additional Software:** Only apps recommended by the school may be downloaded while connected to the school network.
3. **Student-Installed Apps:** Non-academic apps are prohibited.
4. **Software Restore:** The school is not responsible for lost data due to factory resets.
5. **Software Upgrades:** Students must wait for IT department approval before updating major OS versions.

1.4.4.2.6 Acceptable Use

1. **Privacy:** No expectation of privacy exists; all data may be monitored.
2. **Legal Compliance**:
    - Students must adhere to copyright laws and licensing agreements.
    - Possession of hacking software is strictly prohibited.
    - Violations may lead to disciplinary or legal action.
3. **Device Integrity:**
    - iPads: Jailbreaking is prohibited and voids the warranty.
    - Android tablets: Rooting or installing unauthorized firmware is prohibited.
    - VPN apps or software attempting to bypass school network restrictions are not allowed on any device.
4. **Inspection:**
    - Tablets (iPads or Android devices) may be randomly checked by school staff to ensure compliance with policy.

1.4.4.2.7 Protection and Storage

1. **Identification:**
    - Only the school is authorized to mark or label tablets (iPads or Android devices).
2. **Storage:**
    - Tablets must be placed in designated charging stations when not in use.
    - Nothing should be placed on top of a tablet.
3. **Unsupervised Areas:**
    - Tablets must not be left in unsupervised areas (e.g., school grounds, cafeteria, hallways).
    - If found unattended, the device will be taken to the School Safety & Security Department, and disciplinary action may apply.

1.4.4.2.8 Repairs and Replacement

- Students are financially responsible for the repair or replacement of tablets (iPads or Android devices) in cases of damage, theft, or loss.
- If damage is caused due to staff handling or supervision, the school will take appropriate action.

Repair Process:

1. The student must report a lost or damaged tablet to the Class Teacher or IT Department immediately.
2. The student must submit a Tablet Incident Report through the Class Teacher.
3. The school office will contact parents with a damage or loss statement along with the applicable invoice, if any.
4. All repairs must be carried out only at an authorized service center or device manufacturer.

1.4.5 Use of BYOD: Grade 6 – 12 (For Monarch International School)

Note: As per Management decision, the Bring Your Own Device (BYOD) program for Grades 6–12 at Monarch International School is discontinued effective April 2026. From this date onward, the provisions outlined in this section will no longer apply

DPS Monarch International School is committed to fostering a learning environment where students develop essential digital skills, responsible behaviors, and global citizenship. This BYOD (Bring Your Own Device) policy allows students to enhance their learning experience through:

- Digital assessments (Concept Recap)
- Research for project work and ICT
- CISCO Educational Courses

- Student-centered e-learning that emphasizes inquiry and authentic learning
- Online learning tools and digital content

1.4.5.1 General Guidelines

To ensure responsible and effective use of personal devices in the classroom, the following general guidelines outline the expectations for students, parents, and staff regarding the use of Bring Your Own Device (BYOD) at Monarch International School.

1.4.5.1.1 General Guidelines

Students in Grades 6 to 12 may use their personally owned, internet-enabled devices on the school's wireless network with prior teacher or staff approval.

Parental Duties:

- **Device Maintenance:** Ensure devices are charged, updated, and physically protected (e.g., tempered glass, cases).
- **Content Oversight:**
  - Monthly checks for unauthorized apps/games or inappropriate content.
  - Use parental controls (e.g., Apple Screen Time) to restrict non-educational use.
- **Incident Reporting:** Report loss/theft to school authority immediately.

Acceptable Devices:

- Laptops, tablets, iPads, Chromebooks, MacBooks
- Mobile phones and other personal devices are strictly prohibited unless explicitly authorized by school authorities.
- **SIM-enabled devices are strictly prohibited.**

General Conditions:

- The use of personal devices on the school network is a privilege, not a right.
- Parents acknowledge adherence to the school's IT, social media, and Behavior Policies by granting permission for device usage.
- School authorities reserve the right to monitor internet usage and take necessary actions if excessive bandwidth consumption or policy violations occur.

1.4.5.1.2 Device Usage Rules

- **Charging:** Students must bring fully charged devices as charging facilities are limited.
- **Network Connection:** Personal devices may only connect to the school's Wi-Fi; direct wired connections are prohibited.
- **Security:** All devices must have up-to-date antivirus/anti-malware protection. The school is not responsible for data loss due to security threats.
- **Teacher Authority:** Teachers determine when and how devices may be used in class.
- **Disruptions:** Devices must remain in silent mode unless otherwise instructed by the teacher.
- **Internet Access:** Students must comply with internet filtering policies; bypassing school filters is strictly prohibited.
- **Use of VPNs:** The use of VPNs to bypass the school's network is strictly prohibited and may result in losing the privilege of using a device on-premises.
- **Privacy & Respect:** Students may not record, transmit, or post images, videos, or references to others without consent. Any use of devices for bullying or inappropriate content will lead to disciplinary action.
- **Gaming & Illegal Applications:** Playing games on devices is strictly prohibited on campus. The use of any illegal applications, games, or software is strictly prohibited.
- **Printing:** Students cannot connect personal devices to school printers.
- **Security Threats:** Introducing malware or hacking attempts is a severe violation and will result in disciplinary action.
- **App Installations:** Students may only install apps for classroom use with school authorization.

- **Password Management:** Students must not share passwords or access others' accounts.

1.4.5.1.3 BYOD Device Support Limitations

The IT Department will not provide support for BYOD device issues such as forgotten screen passcodes, factory resets, software malfunctions, or operating system errors. Students are responsible for the maintenance and troubleshooting of their BYOD devices. Any such issues must be resolved through external, authorized service providers at the student's or parent's expense.

1.4.5.1.4 Unsupervised Areas

- Devices must never be left unattended in locations such as the playground, cafeteria, library, hallways, or locker rooms.
- Unattended devices will be taken to the Safety & Security Department, and students may face disciplinary action.
- Students should label their devices for easy identification and secure them with strong passwords.
- The school is not responsible for lost, stolen, or damaged personal devices.
- Technical support for personal devices is not provided by the school.

1.4.5.1.5 File and Data Management

- Students are responsible for managing and backing up their own data.
- Important documents should be saved in secure online storage (e.g., OneDrive) or emailed to themselves.
- The school does not guarantee uninterrupted network service and is not liable for data loss due to connectivity issues.

1.4.5.1.6 Consequences/ Legal Propriety

- **Legal Compliance:** Students must follow copyright, trademark, and licensing laws.
- **Hacking & Cybersecurity Violations:** Possession or use of hacking software is strictly prohibited and will result in disciplinary action or legal prosecution.
- **Disciplinary Measures:** Policy violations may lead to loss of BYOD privileges, restricted device use, detention, suspension, or expulsion, depending on the severity of the infraction.

1.4.6 Tablet Charging Stations (For Monarch International School)

All Grade 1 to Grade 5 classrooms are equipped with tablet charging stations to ensure devices are fully charged and ready for use during lessons. The responsibility for the care, arrangement, and safe handling of the charging stations, tablets, and charging cables lies with the respective Homeroom Teachers (HRTs). Although this policy specifically applies to these grades, it is shared with all staff and faculty for awareness.

1.4.6.1 General Guidelines:

1. **Responsibility:**
   - The respective class Homeroom Teachers (HRTs) are fully responsible for the arrangement, supervision, and proper care of the tablet charging stations, tablets, and charging cables assigned to their classrooms.
   - This includes ensuring that all tablets and their charging cables are properly stored and charged when not in use.
2. **Physical Damage:**
   - HRTs will be held accountable for damage to the charging stations or associated components (e.g., cables, adapters) caused by negligence or misuse under their supervision.
   - Any such incidents must be reported to the IT Department immediately for investigation and appropriate action.
   - In cases of negligence or misuse, the cost of repair or replacement of any damaged or missing items will be charged to the responsible HRT.
3. **Locking Mechanism:**
   - Each charging station is equipped with a locking mechanism for added security.

- Keys to the locks are held by the respective HRTs.
- For the safety of the devices, charging stations should only be accessed by the HRT or under their direct supervision.

Note: While this policy is specific to Grade 1 to 5 classrooms, all staff and faculty are encouraged to familiarize themselves with these guidelines for general awareness.

1.4.7 Internet Access Guidelines

DPS Group of Institutions is equipped with modern internet facilities to enhance the learning and administrative processes. The availability of internet access supports educational research, resource sharing, and communication. However, to ensure that the internet is used responsibly and securely, clear guidelines are established for both staff and students. This policy outlines the expectations and restrictions regarding internet usage within the institution, ensuring that school-provided devices and networks are used appropriately for academic and work-related activities, while maintaining the integrity and security of the institution's digital resources. Both staff and students are expected to adhere to these guidelines to foster a productive, respectful, and safe online environment.

1.4.7.1 For School Staff

This policy applies to all staff members who use school-provided devices, networks, and internet access for work-related purposes.

1.4.7.1.1 General Guidelines

1. Internet access is strictly for work-related activities, including research, teaching resources, and administrative functions.
2. Personal use of the internet on school-provided networks and devices is not permitted.
3. The school reserves the right to monitor internet usage, emails, and online activity to ensure compliance.
4. Employees must not share Wi-Fi passwords with unauthorized individuals, including colleagues and visitors.
5. All internet and email communication conducted via school systems is considered school property and subject to disclosure if required.
6. Bypassing the school's network security measures, including using VPNs, proxy servers, or other methods to evade restrictions, is strictly prohibited and will result in disciplinary action.

1.4.7.1.2 Prohibited Activities

Employees must not:

- Access, download, or distribute inappropriate, offensive, or illegal content.
- Use school networks for personal social media, gaming, streaming, or non-work-related browsing.
- Install unauthorized software, including instant messaging apps.
- Share confidential school information or student data outside authorized channels.
- Engage in hacking, phishing, or any activities that compromise network security.
- Send chain letters, spam, or non-work-related solicitations.
- Use the internet for personal financial transactions or business activities unrelated to the school.

1.4.7.1.3 Disciplinary Action

Violations of this policy may result in disciplinary actions, including termination of employment or legal consequences. Employees should seek clarification from the IT Department if unsure about appropriate internet usage.

1.4.7.2 For Students

This policy applies to all students accessing the school's internet and digital resources.

1.4.7.2.1 Acceptable Use Guidelines

1. The internet should be used for educational purposes only, including research, assignments, and school projects.

2. Students must respect the privacy and security of others and should not attempt to access restricted content.
3. School Wi-Fi access is a privilege; misuse may result in restricted access or disciplinary action.
4. Social media access is restricted on school networks unless approved for educational purposes.
5. Students must not share passwords or attempt to bypass security measures.
6. Bypassing the school's network security, including using VPNs, proxy servers, or any unauthorized tools to access restricted content, is strictly prohibited and will result in disciplinary action.

1.4.7.2.2 Prohibited Activities

Students must not:

- Access inappropriate, violent, or illegal websites.
- Use the internet for gaming, social media, or non-educational streaming during school hours.
- Download or distribute unauthorized software, music, or media.
- Engage in cyberbullying, harassment, or sending offensive messages.
- Attempt to hack into school systems or any unauthorized websites.
- Share personal or confidential information online without permission.

1.4.7.2.3 Consequences of Misuse

Any violation of this policy may result in restricted internet access, disciplinary action, or further consequences as deemed necessary by the school administration.

1.4.8 Use of Imaging Devices (Printers, Scanners, Copiers)

- **Ownership and Usage**

  All printing, scanning, and copying devices and materials provided by DPS Group are the property of DPS Group and must be used exclusively for official DPS Group business.

- **Confidentiality Considerations**

  Users must be mindful of their surroundings when printing or copying sensitive or confidential materials. Printed documents containing confidential information should be promptly retrieved from the printer to avoid unauthorized access.

- **Prohibited Actions**

Users are prohibited from the following actions:

  - Moving, removing, or tampering with printers, scanners, or related materials (such as toners or cartridges) without prior approval from the IT department.
  - Attempting to repair or troubleshoot printers or scanners without prior authorization from the IT Service Desk.
  - Printing or distributing inappropriate, offensive, or unethical content.

1.4.9 Use of AI & Emerging Technology

The rise of artificial intelligence (AI), generative tools (such as ChatGPT, Copilot), and other emerging technologies are transforming education and administration. While these tools offer significant benefits in enhancing learning, productivity, and creativity, they also raise concerns around academic integrity, data privacy, and responsible usage. This policy aims to provide clear guidelines to ensure AI and related technologies are used ethically, safely, and in alignment with the institution's values.

1.4.9.1 Purpose

To regulate the ethical and appropriate use of AI tools and emerging technologies in both academic and administrative contexts, in alignment with institutional values and data protection policies.

1.4.9.2 Definitions

- **Artificial Intelligence (AI):** Technology that simulates human intelligence processes such as reasoning, learning, and decision-making.
- **Generative AI:** Tools that can produce original content (e.g., text, images, audio, or code) based on prompts or input data (e.g., ChatGPT, DALL·E, Copilot).
- **Emerging Technologies:** Innovative digital tools that are still evolving and may impact teaching, learning, or operations.

1.4.9.3 Guidelines:

For Students:

Allowed Uses:

- AI tools may be used with teacher approval for:
  - Brainstorming or idea generation
  - Grammar and spelling correction
  - Research assistance
- AI-generated content must be clearly cited (e.g., *"This content was generated using ChatGPT."*).

Prohibited Uses:

- Submitting AI-generated content as original work (e.g., essays, assignments) without proper citation—considered academic dishonesty.
- Using AI to solve exam questions, bypass assessment processes, or mimic human responses in evaluations.

For Staff:

Administrative Use:

AI tools may support:

- Drafting lesson plans, reports, assessments, or instructional material
- Content creation and planning
- Communication or workflow support

All outputs must be reviewed for accuracy and appropriateness before use.

Prohibited Uses:

- Entering, storing, or sharing personally identifiable or sensitive data (e.g., student names, grades, IDs, health records) on public or non-approved AI tools.
- Over-reliance on AI-generated outputs without human verification.

1.4.9.4 Consequences:

- **Students:** Violations of this policy will be handled as academic misconduct under the school's disciplinary code.
- **Staff:** Misuse may lead to **disciplinary actions** in accordance with institutional HR procedures, up to and including formal warnings or suspension of access privileges.

1.4.10 Email and Electronic Platform Use Policy (Office 365 Email)

This policy governs the use of electronic mail (email) services provided by DPS Group, including Office 365 Email and other electronic platforms used for official business communications. All users of DPS Group-provided email accounts, including students, faculty, staff, consultants, and contractors, must adhere to the terms outlined below.

Ownership & Management

- DPS Group owns licenses for email accounts and retains full ownership of the contents of email mailboxes created for conducting official DPS Group business. This includes mailboxes for faculty, staff, consultants, and contractors.
- The IT department is responsible for managing and supporting the email infrastructure and services of DPS Group.

Access to Email Accounts

The IT department may provide access to, or copies of, email contents as required for DPS Group business or during security forensic investigations.

Disabling of Email Accounts

Email accounts may be disabled under the following circumstances:

- When an employee's affiliation with DPS Group ends. Exceptions may be granted if access is required to fulfill a business need or if authorized by the Principal or Management.
- In cases of security incidents, including SPAM or inappropriate use of email.

1.4.10.1 Email Use Guidelines for Employees

Employees are expected to adhere to the following standards regarding email usage:

- Restrict the use of DPS Group email accounts to school-related communication only.
- Do not use DPS Group email for personal activities, such as registering on online sites.
- Do not forward DPS Group emails to non-DPS Group systems (e.g., personal cloud-based email services).
- Avoid making offline copies of email contents that may expose sensitive information to unauthorized disclosure.
- Do not retain copies of emails once their affiliation with DPS Group ends.

1.4.10.2 General Guidelines for All Email Users

- Users must not share passwords, credit card details, or any sensitive data through email without proper protection, such as encryption.
- Offensive, abusive, violent, threatening, or harmful content must not be transmitted via email.
- Internal emails, particularly those containing confidential or classified information, must not be shared outside of DPS Group or posted on social media platforms.
- Chain emails should not be transmitted or forwarded within or outside DPS Group.
- Users must not falsify or impersonate sender addresses in emails.
- Users must not present themselves as representing DPS Group or any of its units when communicating with external parties unless explicitly authorized.
- Take necessary precautions to avoid phishing attacks and other email-related threats.
- Users must not bypass email access controls.
- Any irregularities or suspicious activities must be reported to IT for investigation.
- Mail broadcasting for personal, commercial, or non-DPS Group-related communication is prohibited.
- Mass emails should only be sent if relevant to all recipients. Email addresses or phone numbers should not be exposed to third parties or groups.

1.4.10.3 Bulk Email and Mailing List Usage

- DPS Group provides mailing lists to facilitate communication with large groups, such as students or parents. However, users must exercise caution when sending bulk emails:
  - Bulk emails and mailing lists may only be used for official DPS Group-related topics. Personal, commercial, or non-school-related communications are prohibited.
  - Emails sent through mailing lists should be relevant to the specific audience. Avoid mass emails unless the content is pertinent to all recipients.

- Users must consider the appropriateness of the content before sending bulk emails. Mailing lists must not be used for spam, unsolicited emails, or content that is offensive or harmful.
- Advertising of personal achievements, properties, cars, etc., is not allowed unless using a dedicated mailing list or group approved by the Principal and Management.

By adhering to these guidelines, all DPS Group members help ensure the responsible and secure use of email services for official communication and prevent misuse or harm to the institution's operations and reputation.

1.4.11 Use of Network Access

Users accessing the DPS Group Network are expected to use network resources in a responsible, ethical, and secure manner. The following guidelines apply specifically to the use of network access:

1. **Prohibited Content**
   Users shall not knowingly download, access, or share malicious, offensive, abusive, profane, illegal, or harmful content that could compromise the DPS Group network or resources.
2. **Peer-to-Peer File Sharing**
   Due to security risks, users should avoid using peer-to-peer file sharing protocols. Any exceptions to this policy must be requested and authorized by the IT department following a thorough assessment.
3. **Unauthorized Network Configuration**
   Users shall not install, configure, or modify any network components, devices, or software without prior consent from the IT department. This includes:
   a. DPS Group network equipment (wired or wireless)
   b. Network servers (e.g., DHCP, DNS, etc.)
   c. Devices or applications that consume excessive network bandwidth
   d. Devices, software, or applications that bypass security mechanisms
4. **Bypassing Security Controls**
   Users shall not attempt to bypass the security mechanisms implemented by DPS Group, including firewalls, VPNs, and other protective measures, when accessing the network.
5. **Unauthorized Access Devices or Software**
   Users should not install or use devices or software that allow direct access to their systems or devices without going through the existing security controls, such as VPN or firewalls. Unauthorized access methods, such as modems or remote access software, are strictly prohibited.
6. **Liability for Damages**
   Users are solely responsible for any indirect, consequential, special, or punitive damage or losses resulting from inappropriate use of network access.
7. **Requests for Access Modifications**
   Users may submit requests for adjustments to content filtering or network access restrictions to the IT Department. The IT department will assess the potential risks and retain the right to deny any requests that could jeopardize the security of the network or DPS Group's resources.

By following this policy, users contribute to a safe, secure, and efficient network environment at DPS Group.

1.4.11 Use of Closed-Circuit Television (CCTV)

The purpose of this policy is to regulate the management, operation, and use of the closed-circuit television (CCTV) system at DPS Group of Institutions. The CCTV system consists of multiple fixed cameras located within and around the DPS Group of Institutions premises. These cameras are managed and controlled by the IT and Security departments, with access restricted to authorized personnel.
This policy will be reviewed periodically by the Management Team, Head of Security, Head of IT, and other relevant parties as necessary.
The DPS Group of Institutions CCTV system is intended for the following purposes:

- Monitoring school operations and ensuring security.
- Protecting DPS Group of Institutions property and assets.
- Retaining and utilizing recorded images as evidence when required.

1.4.12.1 IT Department Responsibilities

The IT Department has the authority to view, monitor, and control the operational CCTV cameras.

- Any new camera requests or changes that impact operations or the monitoring of existing cameras must be initiated and approved by the Facilities Department before being forwarded to the IT Department for technical review and/or implementation.
- The Facilities Department is authorized to retrieve recorded video footage in coordination with the IT Department, following formal approval from Management or the Principal.
- The IT Department will coordinate all technical aspects related to CCTV systems with the Facilities Department and third-party vendors supporting DPS Group.

1.4.12.2 Safety and Security Department Responsibilities

- The Safety and Security Department has the authority to view, monitor, control, and retrieve footage from security-related CCTV cameras only.
- Any requests for new cameras or changes affecting security operations or existing camera monitoring must receive prior approval from the Safety and Security Department before being forwarded to the Telecom Division for technical review and/or implementation.
- The Safety and Security Department may retrieve recorded footage from security cameras, in coordination with the IT/Telecom Division, when necessary.
- Any department requesting access to recorded data must obtain authorization from the Emergency Response & Security Manager.

All operators and supervisors involved in CCTV monitoring are required to perform their duties in accordance with this policy. CCTV systems are considered essential business tools and must be handled responsibly, ensuring respect for privacy expectations among DPS Group staff.

CCTV system usage is restricted to safety and security purposes only. Misuse of these systems may lead to disciplinary action.

1.4.12.3 Camera Placement

The siting of cameras will be determined by the Facilities Department, in accordance with operational requirements.

- Signs must be placed at all entry points and key areas of the DPS Group premises to notify personnel, contractors, and visitors that CCTV surveillance is in operation. The signage design will be approved by the Safety Department.

1.4.12.4 Image Quality

It is essential that the images captured by DPS Group of Institutions' CCTV cameras are clear and of sufficient quality to serve their intended purposes, as outlined by the Safety and Security Department.

1.4.12.5 Maintenance and Service

Upon installation, all CCTV equipment must be thoroughly tested to ensure proper functioning.

- Regular service and maintenance of the CCTV system should be coordinated with the IT Department to ensure the continued reliability and effectiveness of the system.

1.4.12.6 Integrity of Recordings

The integrity of CCTV recordings must be preserved to maintain their evidential value and to protect the privacy rights of individuals captured in the footage. Access to recordings and the security of such images must be managed according to DPS Group of Institutions' security policies.

1.4.12.7 Storage of Digital Recordings

CCTV recordings must be digitally stored in secure systems within DPS Group of Institutions. The minimum retention period for all recordings is 30 days. Recorded footage will be automatically erased after 30 days unless there is a specific reason to retain it for a longer period.

1.4.12.8 Viewing of Images

Viewing of CCTV images is restricted to authorized personnel only. Unauthorized viewing or sharing of images is prohibited, except for maintenance and servicing purposes.

1.4.12.9 Access to and Disclosure of Images to Third Parties

Access to recorded CCTV images by unauthorized third parties is strictly prohibited. Disclosure to third parties may only occur under controlled conditions to preserve individual rights and the integrity of the evidence for potential legal proceedings.

1.4.12.10 CCTV Recording Retrieval and Dissemination

- CCTV recordings will be made available for investigation by HR, Facilities, Safety and Security, and Safety Departments as necessary.
- Recordings may also be provided to local law enforcement authorities when required, with approval from HR, Facilities, and Safety and Security Departments.
- Requests for retrieval of CCTV footage can be made through the Safety and Security Division by submitting a Service Request. All retrieval requests must be approved by the Principal and the Facilities Manager.
- Recorded footage will be handled by DPS Group Security and will not be shared externally without prior approval from the Principal, Facilities Manager, or Management.

1.4.12.11 CCTV Cameras Recording Retention

CCTV systems generate large amounts of data. The required storage space depends on the compression ratio, the number of images captured per second, and image size. To manage storage effectively, recordings for each camera will be retained for no longer than 30 days unless they are part of an ongoing investigation, or if retention is specifically requested.

1.4.13 Use of Telecommunication Services (Telephones)

DPS Group of Institutions utilizes IP phones (hardware and software) to provide efficient and effective telephone services to its employees. All users are expected to comply with the following guidelines to ensure proper handling, security, and accountability of the phone systems.

1.4.13.1 General Responsibilities

a. Care and Maintenance
Users must handle IP phones with care. Any hardware or configuration issues should be promptly reported to the IT Department for resolution.

b. Emergency Phones
Emergency phones should be used solely for emergency purposes. Misuse of these phones will not be tolerated.

c. Phone Return
Upon completion of their employment or during the exit clearance process, users must return their IP phone hardware to the IT Department.

1.4.13.2 Phone Condition and Reporting

- **Loss of Phone**
  If an IP phone is lost, the user must immediately report the loss to the IT Department. The cost of the replacement phone will be charged to the respective department's cost center.
- **Damage to Phone**
  In the event that an IP phone is damaged, users must immediately notify the IT Department for necessary action. If damage occurs through misuse or negligence, the cost of replacement or repair will be the responsibility of the user.
- **Phone Relocation**
  Users must not relocate their office phone without prior approval from the IT Department. Unauthorized relocations can disrupt services and should be avoided.

1.4.13.3 Cost Control and Usage Monitoring

- **Responsible Usage**
  All users are expected to use the telephone system responsibly and minimize costs wherever possible. Excessive or unnecessary usage may be subject to review.
- **Managerial Oversight**
  Line Managers are responsible for ensuring that telephone usage within their teams is strictly for business purposes. Managers should monitor and control usage to ensure compliance with the policy.

1.4.13.4 Office Telephone Procedure

DPS Group reserves the right to monitor the use of telephone facilities through appropriate mechanisms and may deactivate phone services if necessary. Additionally, the institution maintains the right to collect telephone sets when required.

1.4.13.4.1 Provision of Phones

- **Request Process:** All requests for office telephones must be submitted by completing an IT Material Requisition Form. Approval from both the Line Manager and Principal is required before processing the request.
- **Activation of Outgoing Calls:** Outgoing call functionality will only be activated after the completion of the IT Material Requisition Form. and receiving prior approval from both the Line Manager and Principal.

1.4.13.4.2 Installation and Office Extension

- **Installation:** The IT Department will purchase, install, and configure the office telephone at the requested user's designated location, with approval from both the Line Manager and Principal.
- **Office Extension:** Each entitled user will be assigned a unique office extension number. This number will remain unchanged unless strong justification is provided, and approval from both the Line Manager and Principal is required for any changes.

1.4.13.4.3 Deactivation

To deactivate phone services, the end user must submit an official request with approval from both the Line Manager and Principal. The request should be forwarded to the IT Department for processing.

1.4.14 Use of Social Media

At DPS Group, employees and users are expected to maintain professionalism and uphold the reputation of the organization when engaging in any form of social media activity. The following guidelines apply to both personal and professional use of social media:

1.4.14.1 General Guidelines

- **Sharing Information:** DPS Group information should not be shared via social media platforms.
- **Work-related Communication**: Personal accounts must not be used to communicate work-related matters.
- **Linking to DPS Group:** Users should avoid posting content or images that directly or indirectly associate them with DPS Group unless authorized.
- **Excessive Use:** Excessive use of social media during work hours is prohibited.
- **Representation of DPS Group:** Employees must not represent DPS Group on any social media platform without explicit authorization.
- **Cultural Sensitivity:** Content that is offensive or harmful to the local community or Qatari culture should not be shared or liked. Violation of this may result in disciplinary actions.

1.4.14.2 Professional and Personal Use

- **Reputation and Image:** Stakeholders should be aware of how their social media activities affect their personal reputation and the image of DPS Monarch International School. Posts may remain public for a long time and influence perceptions of the school.
- **Monitoring of Public Content:** DPS Monarch International School may observe publicly available content on social media platforms. Stakeholders should exercise good judgment and avoid posting inappropriate or harmful material related to the school.
- **Prohibited Content:** Stakeholders are prohibited from posting defamatory, pornographic, harassing, or libelous content, or anything that may create a hostile work environment.
- **Confidentiality:** No confidential or sensitive information related to DPS Monarch International School should be published without prior approval. Any uncertainty about confidentiality should be clarified with the principal or Headmistress.
- **Media Inquiries:** If stakeholders receive inquiries from the press or media, they should redirect them to authorized spokespersons of DPS Monarch International School.
- **Handling Disputes:** In case of online disputes or antagonistic situations, stakeholders should politely disengage and seek guidance from the principal.
- **Permission for Images:** Stakeholders must obtain appropriate permissions before using images of current or former staff, students, vendors, or other stakeholders. They should also get permission to use copyrighted material, trademarks, or intellectual property owned by third parties.

1.4.14.3 Social Media Usage at Work

- **Work-related Use:** Social media use during working hours should be limited to business purposes. Personal use of social media or blogging is discouraged on school devices, and excessive personal use may lead to disciplinary action.
- **After-Hours Conduct:** Social media activity outside of work hours that violates the school's Code of Conduct or other policies may result in disciplinary action, including termination.
- **Disclaimers:** If stakeholders publish content that relates to DPS Monarch International School, they should include a disclaimer: "The opinions and content expressed here are my own and do not represent DPS Monarch International School's positions, strategies, or opinions."
- **Separation of Accounts:** It is recommended that stakeholders keep personal and school-related social media accounts separate, ensuring that DPS Monarch International School's image is always respected.

1.4.14.4 Legal and Privacy Considerations

- **Offensive Content:** Any offensive material directed at stakeholders may result in the involvement of Qatari government authorities for legal action as per local laws.
- **Use of Photos and Videos:** The school may post photos and videos of students, teachers, and staff for educational purposes, such as newsletters, yearbooks, or school websites. These materials will be handled according to Qatar's privacy laws. If stakeholders have concerns or objections to the use of photos or videos, they should contact the school office.

This policy ensures that the use of social media is aligned with DPS Monarch International School's values and legal obligations while protecting the privacy and safety of all stakeholders.

1.4.15 Use of Cloud Services

Staff are permitted to use the DPS Group's licensed cloud services (OneDrive), provided that a risk assessment is conducted prior to utilizing public cloud-based IT services for DPS Group-related business. The IT Department is available to assist in conducting these assessments and will offer guidance based on compliance, security, and operational considerations.

1.4.16 Use of File Storage (File Shares)

Users of the shared file storage services must adhere to the following guidelines:

1.4.16.1 Departmental Shares

- Each department and its respective Head of Department (HOD) are responsible for authorizing access and managing the content of their designated shared folders.
- Departmental shared folders should undergo periodic reviews by the HOD and Academic Coordinator to ensure content validity and proper access control. The IT Department can assist with these tasks but is not liable for any issues or findings that arise.
- Departmental shares are not to be used for backing up personal or individual user documents.
- Access to departmental shares is restricted to devices that are managed by DPS Group. Personal devices are not permitted to access these shared folders.

1.4.16.1 Individual Shares

- Users are prohibited from storing illegal or inappropriate content in individual shares.
- To maintain the security of their stored content, users should back up files from individual shares to offline storage devices. The IT department cannot ensure that such content will be backed up to central backup facilities.

1.4.17 Use of Web/Portal Services

1. Users who upload or post content to DPS Group's web servers or portals are fully responsible and accountable for the content they provide.
2. Any data classified as Internal, Limited Access, or Restricted must not be shared via DPS Group's websites or portals unless appropriate security measures are in place.
3. Access to DPS Group's portal and web services will be revoked once a user's affiliation with the institution ends (e.g., when the user is no longer a faculty member, staff, or student). However, alumni accounts will remain active to facilitate access to alumni communities. Exceptions to this policy can be made with proper authorization.

1.4.18 Use of Audiovisual and Classroom Technology

The IT Department manages and deploys audiovisual (AV) and classroom technology (CT) equipment. These resources are the property of DPS Group and must be handled with care and responsibility.

1. AV and CT resources may only be used for conducting DPS Group business or academic purposes.
2. Smart classroom technology is generally restricted to faculty members. Students may only use such technology for academic purposes with prior approval from the Class Teacher/HRT or Academic Coordinator. Any usage by students must be supervised by a faculty member.
3. Users are prohibited from attempting to repair AV/CT equipment. Any malfunctions or issues must be reported to the IT department.
4. Users are not permitted to dismantle or move AV/CT equipment without prior authorization from the IT Department.
5. Access to smart classroom technology systems is secure and should only be used for teaching purposes.
6. Students are prohibited from using smart classroom technology for non-academic purposes or outside of designated class hours.

7. Faculty, staff, and students must not attempt to dismantle or move any smart classroom technology systems without notifying the IT department and obtaining authorization.

1.4.19 Expectation of Privacy

DPS Group respects user privacy; however, it reserves the right to access and review data transmitted across its network under specific circumstances. These include, but are not limited to:

1. Compliance with legal or regulatory requirements.
2. Participation in legal investigations were required.
3. Investigation of security incidents.
4. Accessing employee emails or files for the purpose of conducting DPS Group business (e.g., accessing the emails of former employees).

In some instances, users may not be notified of the disclosure or access to their information.

1.4.20 Compliance with Cyber Rules

Users of DPS Group's IT resources must:

1. Adhere to all applicable laws and regulations, including the Qatar Cybercrimes Law.
2. Follow all copyright laws and licensing agreements related to digital resources, including software, multimedia files, and other digital content.
3. Not use, copy, or distribute copyrighted works (such as web graphics, multimedia files, trademarks, software, and logos) without legal authorization.

Failure to comply with this policy may result in:

1. Revocation of access to DPS Group IT resources, including wired and wireless network services.
2. Disciplinary and/or legal action in accordance with DPS Group policies and relevant local laws and regulations.