Notice of Using Personal Computers

Notice of using personal computers at Cigu Elementary School

1. Do not use unauthorized computer software.
2. Do not dismantle or install additional computer devices arbitrarily.
3. Do not make unauthorized changes to the system environment settings.
4. Update the password at least every 3 months and the password length should be a minimum of 8 characters.
5. Do not use the computer for unauthorized actions, including personal or commercial purposes.
6. Keep the computer clean at all times and wipe it at least once a week.
7. Do not place water, beverages, small stationery, or any other objects near the computer to prevent damage to the equipment.
8. Scan every external file for viruses before opening. Do not remove or turn off the antivirus software arbitrarily.
9. Shut down the computer under normal procedures before leaving work.
10. **Update software and keep the systems up to date to prevent security issues. Do not disable the automatic update programs of the system arbitrarily.**
11. Set the security level of browsers to “Medium High” or higher such as Internet Explorer. Contact the Information Center for Internet security inspection and management if you need to lower the security settings to run specific programs.
12. Turn off the preview function on the email software. Do not open any emails from unknown sources.
13. Set up a screen saver program with password protection. The screen saver activation time should be set to within 10 minutes.
14. Avoid enabling network file and folder sharing through My Network Places and make sure to disable the Guest account.
15. Do not download or install computer software from unknown sources, software that is unrelated to our school's business, or any software that may cause concerns regarding legal compliance, including copyright or intellectual property infringement.
16. Set the security level of Macro to “High” or higher on Microsoft Office software,

including Word, Excel, PowerPoint, etc. Contact the Information Center for Internet security inspection and management if you need to lower the security settings to run specific programs.

17. Do not use peer-to-peer (P2P) software and tunneling software to download or share files.
18. Do not use instant messaging applications, such as MSN, Yahoo Messenger, etc. during working hours. Permission is required if it is necessary for work purposes. Supervisors from different divisions should closely monitor the usage of instant messaging by the staff.
19. Do not browse inappropriate websites, including violent, pornographic, gambling, hacking, malicious websites, phishing scams, botnets, etc. during work or class hours, as well as browsing non-work-related websites, to avoid internal bandwidth congestion. Supervisors from different divisions should closely monitor Internet usage by the staff.
20. Do not use external web-based email services, such as Webmail. Supervisors from different divisions should closely monitor Webmail usage by the staff to prevent security issues.
21. Do not transfer MP3, pictures, files, or non-work-related content via the Internet or use streaming media during working hours. Do not affect the network performance of the primary operation system in non-working hours, such as lunch breaks or after work.
22. The staff's internet usage should prioritize not affecting the network performance of the primary systems. In case of resource conflicts, priority will be given to the main systems of our institution.
23. Backup important data files on computers regularly to prevent data loss.
24. Store confidential and sensitive files and data on isolated devices, disconnected from external networks.
25. Our institution conducts irregular internal inspections throughout the year. If any misconduct or violations are found, the staff will be subject to disciplinary measures in accordance with our institution's rules and regulations.
26. Do not set up personal websites for school divisions, except for the necessary official division websites. This measure is taken to prevent hacker attacks and to ensure compliance with relevant domestic laws and regulations.