Republic of the Philippines
Department of Education
CORDILLERA ADMINISTRATIVE REGION
SCHOOLS DIVISION OF BAGUIO CITY

DepED DIVISION OFFICE BAGUIO CITY
RELEASED
NOV 11 2026
By:
Time: CTRL No.:

November 11, 2026

DIVISION MEMORANDUM
No. 771-2026

DISSEMINATION OF RM NO. 912.2026 "MANDATORY CYBERSECURITY MEASURES AND DATA PROTECTION SAFEGUARDS ON THE USE OF OFFICIAL DEPED EMAIL ACCOUNTS"

To: Assistant Schools Division Superintendent
Chief Education Supervisors
Public Schools District Supervisors
Public School Heads
School Administrative Officers
All Others Concerned

1. Enclosed is Regional Memorandum No. 912.2026 titled "Mandatory Cybersecurity Measures and Data Protection Safeguards on the Use of Official DepEd Email Accounts."

2. All concerned are directed to strictly observe and comply with the mandatory cybersecurity measures and data protection safeguards prescribed in the said Memorandum

3. For information and strict compliance.

SORAYA T. FACULO PhD, CESO V
Schools Division Superintendent

For the Schools Division Superintendent:

NIEVES D. EBANIO
Administrative Officer V

OSDS/STF/nde

DepED
SDO Baguio City
OSDS-AS-Records Unit
RECEIVED
Date: NOV 11, 2026 | Time: 08:39 AM
Received By: Jet

Republic of the Philippines
Department of Education
CORDILLERA ADMINISTRATIVE REGION

DEPARTMENT OF EDUCATION
RECORDS SECTION, REGIONAL OFFICE - CAR
RECEIVED
NOV 11 2026
BY: TIME 1:51

November 10, 2026

REGIONAL MEMORANDUM
No. 912. 2026

MANDATORY CYBERSECURITY MEASURES AND DATA PROTECTION SAFEGUARDS ON THE USE OF OFFICIAL DEPED EMAIL ACCOUNTS

To: Assistant Regional Director
All Schools Division Superintendents
All Regional Office Chiefs/OICs
All Schools Heads
All Teaching and Non-Teaching Personnel
All Others Concerned

1. The Department of Education – Cordillera Administrative Region (DepEd CAR) Regional Office **highlights the urgent need for heightened cybersecurity awareness and personal data protection** among all personnel. Recent reports indicate an increase in sophisticated phishing scams, credential harvesting, and financial fraud targeting DepEd personnel, resulting in data breaches and personal financial losses due to compromised accounts.

2. To prevent potential security breaches and ensure system integrity, all personnel are directed to strictly adhere to the following mandatory cybersecurity safeguards:

a. Prohibited Use of Official Email for Personal Transactions. Pursuant to DepEd Memorandum No. 227, s. 2012 (Guidelines on the Use of the DepEd Email Service) and OUA Memo 00-0820-0130 (Guidelines on the Use and Administration of G Suite and Microsoft 365 for Education), the official *deped.gov.ph* email account is a government email service obtained in the interest of public service designated solely for official communications, institutional tasks, and work-related platforms. It must not be used in connection with any commercial, religious, social, political and other similar interests —including personal online banking, online shopping, or private social media registrations.

b. Protection of Account Access (Prohibition on Credential Sharing). Pursuant to **OUA Memo No. 01-1019-0386** (Sharing of DepEd Email and Password), account credentials and passwords are strictly confidential and non-transferable. Personnel are strictly prohibited from sharing, delegating, or surrendering their DepEd email login credentials to colleagues, private lending institutions (PLIs), or third-party organizations.

c. Warning Against Fake Land Bank Emails (Phishing). Land Bank of the Philippines (LBP) will never send emails requesting personnel to click links to update passwords, unlock accounts, or verify personal details. Any email claiming to be from Land Bank requiring link validation is a fraudulent

attempt to compromise financial accounts. Personnel are directed to immediately report such messages as **Phishing** within their DepEd email interface without clicking any links or downloading attachments.

d. Enforcement of Strong and Multi-Factor Authentication (MFA). All personnel are required to adopt strong password standards and enable Multi-Factor Authentication (MFA/2FA) on their official @deped.gov.ph accounts. Passwords must be at least twelve (12) characters in length, combining uppercase and lowercase letters, numbers, and special characters. Passwords must not contain easily guessable personal information, such as names, birthdates, or employee numbers. Furthermore, personnel are strongly advised to update their passwords periodically.

e. Caution on Unverified Links and Attachments. Personnel must exercise high vigilance when handling emails received from unknown or external senders. Do not click embedded links or download attachments from messages that convey artificial urgency, threaten account suspension, or offer unsolicited rewards. Personnel must verify the sender's actual email domain and address prior to replying or interacting with message contents to prevent unauthorized system access and credential harvesting.

3. All Heads of Offices and School Heads are directed to ensure that all teaching and non-teaching personnel under their supervision understand and practice these safeguards to maintain collective cybersecurity protection across the region.

4. Should there be queries or technical clarifications, please contact the Regional Information and Communications Technology Unit (ICTU) through email at **car.ictu@deped.gov.ph**.

5. Immediate dissemination and strict compliance with this Memorandum is desired.

Digitally signed by
Capulong Nicolas Tongol
Date: 2026.11.10
09:38:48 +08'00'

NICOLAS T. CAPULONG PhD, CESO III
Director IV/ Regional Director