Regional Memorandum
No. 429 s. 2023

MANAGING SOCIAL MEDIA ACCOUNT/S OF SCHOOLS AND FIELD OFFICES AND INCIDENT REPORTING

To
- Schools Division Superintendents
- Designated Division Information Officers
- Division Information Technology Officers
- Principals and Schools Heads
- Designated School Information Officers
- ICT Coordinators

1. Due to the increasing online hacking incidents of official Facebook pages of Department of Education offices and schools, this office, through the Information and Communication Technology Unit (ICTU) and the Public Affairs Unit (PAU), releases the Social Media Management, Privacy and Security, and Incident Report Submission Procedures.

2. Schools Division Offices (SDOs) and public schools are hereby advised to strictly obey the following:
   a. Creating a safe and welcoming social media page
      - i. Share photos and videos that you own the right to share
      - ii. Post appropriate content
      - iii. Foster meaningful and genuine interactions
      - iv. Follow community standards and existing DepEd issuances
   b. Managing Social Media Account
      - i. Pin important posts to the top of your page
      - ii. Manage individual comments
      - iii. Block offensive language
      - iv. Hide impolite and improper words in comments
      - v. Pin your favorite comments
   c. Privacy and Security
      - i. Secure Strong Password
      - ii. Apply two-factor authentication
      - iii. Review Page roles and permissions
      - iv. Watch out for suspicious links and malicious software
      - v. Never share your login information
      - vi. Make sure to log out of Facebook when using a public computer you share with other people
vii. Limit your Official Facebook page administrators to two (2) trusted personnel
viii. Be sure to remove the additional temporary admin account once live streaming is done.

3. SDOs and public schools are instructed to submit an incident report of online hacking incidents together with an action plan to be taken, within 12 hours after the online hacking occurred. Send these incident reports and action plans to ICTU and PAU through email at ict.calabarzon@deped.gov.ph and pau.calabarzon@deped.gov.ph. Moreover, the incident must be reported directly to the nearest/available Cybercrime Division for appropriate action. The SDOs and schools may coordinate with their local Cybercrime Division for contact details. Attached hereto is the Incident Report and Action Plan templates to be used.

4. Strict compliance with this memorandum is desired.

cc: ict-il

ATTY. ALBERTO T. ESCOBARTE, CESO II
Regional Director
<table>
<thead>
<tr>
<th>School ID</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>School Name</td>
<td>SDO</td>
</tr>
<tr>
<td>Type of Incident</td>
<td>Date/Time Incident</td>
</tr>
<tr>
<td>School Head Name</td>
<td>Contact No.</td>
</tr>
<tr>
<td>FB Page Administrator</td>
<td>Contact No.</td>
</tr>
</tbody>
</table>

**Description of Incident:**

Prepared by:

FB Page Administrator

Noted:

School Head

Recommended

Schools Division Superintendent
Type of Incident:
Date/Time of Incident:
Person Responsible/s:

<table>
<thead>
<tr>
<th>Plan of Action/Activity</th>
<th>Timeline</th>
<th>Person Responsible</th>
<th>Office/s Concerned</th>
<th>Status/Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prepared</th>
<th>Noted:</th>
<th>Reviewed:</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>FB Page Administrator</td>
<td>School Head</td>
<td>Division Information Technology Officer</td>
<td>School Division Superintendent</td>
</tr>
</tbody>
</table>