



Internal Audit

Social Network Management Audit

Social Network Management Audit

Table of Contents

Executive Summary	3
Background	5
Scope	9
Objective.....	9
Methodology.....	10
Audit Observations and Recommendations	11
Observation 1 – Processes, procedures, and controls surrounding authorization, administration, and management of District affiliated social media accounts could be enhanced	11
Observation 2 – Rules and requirements for configuring District affiliated social media account security/privacy settings should be implemented.....	15
Observation 3 – Guidelines for managing District affiliated social media content should be enhanced	17
Observation 4 – District affiliated social media accounts should be easily identifiable, communicated, and promoted.....	19
Conclusion	22
Attachment 1	23
Definition of Risk Level.....	23
Attachment 2	24
Management Response	24

Date: February 14, 2024

To: Board of Trustees
Stephanie S. Elizalde, Ed.D., Superintendent

From: Robert Rubel, MBA, CPA, CIA, CISA
Chief Internal Audit Officer

Subject: Social Network Management Audit

Executive Summary

The Dallas Independent School District (District) Office of Internal Audit (OIA) has completed the Social Network Management Audit.

The audit focused on the usage of official District and District affiliated social networks¹ and web services. The audit included reviewing processes and controls surrounding management of District affiliated social media accounts² primarily at the campuses, including administrative roles and responsibilities, content management, security controls, and strategy. Auditors also reviewed the District's processes and controls surrounding the management of campus websites.

The Communication Services Department is tasked with overseeing social media management for the District. The department currently maintains the content and engagement for the central District accounts; however, the individual departments and campuses are responsible for managing their District affiliated social media accounts as well as the content posted to them.

The District's Communication Services Department has been recognized as one of the industry's leaders in education publications, e-newsletters, digital media programs, radio/TV/video programs, podcasts, social media, infographics, blogs, and websites.

Overall, Communication Services is working to further develop processes to strategically manage social media and web services to provide efficient and effective communications that engage students, parents, employees, and community members.

¹ All information noted throughout the report regarding social media platforms and their capabilities is relevant as of June 22, 2023. Readers should be aware that certain information could have changed from this date.

² For the purposes of this report, "official District social media accounts" refers to the main social media accounts for the District, and "District affiliated social media accounts" refers to campus-based or departmental accounts, profiles, pages, groups, etc. created by District staff for the purpose of representing a Dallas ISD function, organization, campus, etc. This would not include accounts, profiles, pages, or groups created by individuals who are not Dallas ISD staff, such as PTA, PTO, alumni pages, fan pages or pages not managed by a Dallas ISD team member.

Opportunities for improvement were identified in the following areas:

1. Processes, procedures, and controls surrounding authorization, administration, and management of District affiliated social media accounts could be enhanced.
2. Rules and requirements for configuring District affiliated social media account security/privacy settings should be implemented.
3. Guidelines for managing District affiliated social media content should be enhanced.
4. District affiliated social media accounts should be easily identifiable, communicated, and promoted.

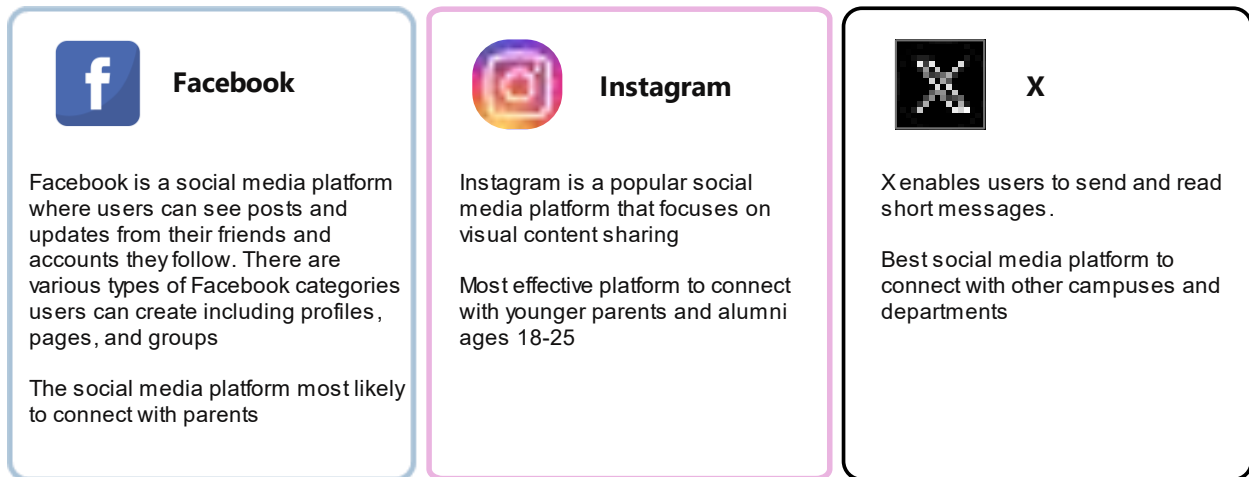
Implementation of the recommendations in this report could assist Communication Services in strengthening governance of District affiliated social media accounts.

Background

Social Media Management

Social media has rapidly revolutionized the way individuals, businesses, and organizations communicate. Social media, if well managed, provides the tools and resources to enhance brand awareness and engagement with the public. Online communication has the ability to easily and quickly reach large audiences. Additionally, it allows for a generally less-expensive form of advertising or marketing. There are many types of social media, from blogs to photo-sharing sites to instant messaging or video-sharing portals. Currently, the District utilizes four primary social media platforms. Facebook, Instagram, X³, and YouTube⁴. These platforms are used for districtwide accounts as well as for individual campuses, groups, events, etc.

The following graphic provides general information on each of the platforms.



Social Media Administration

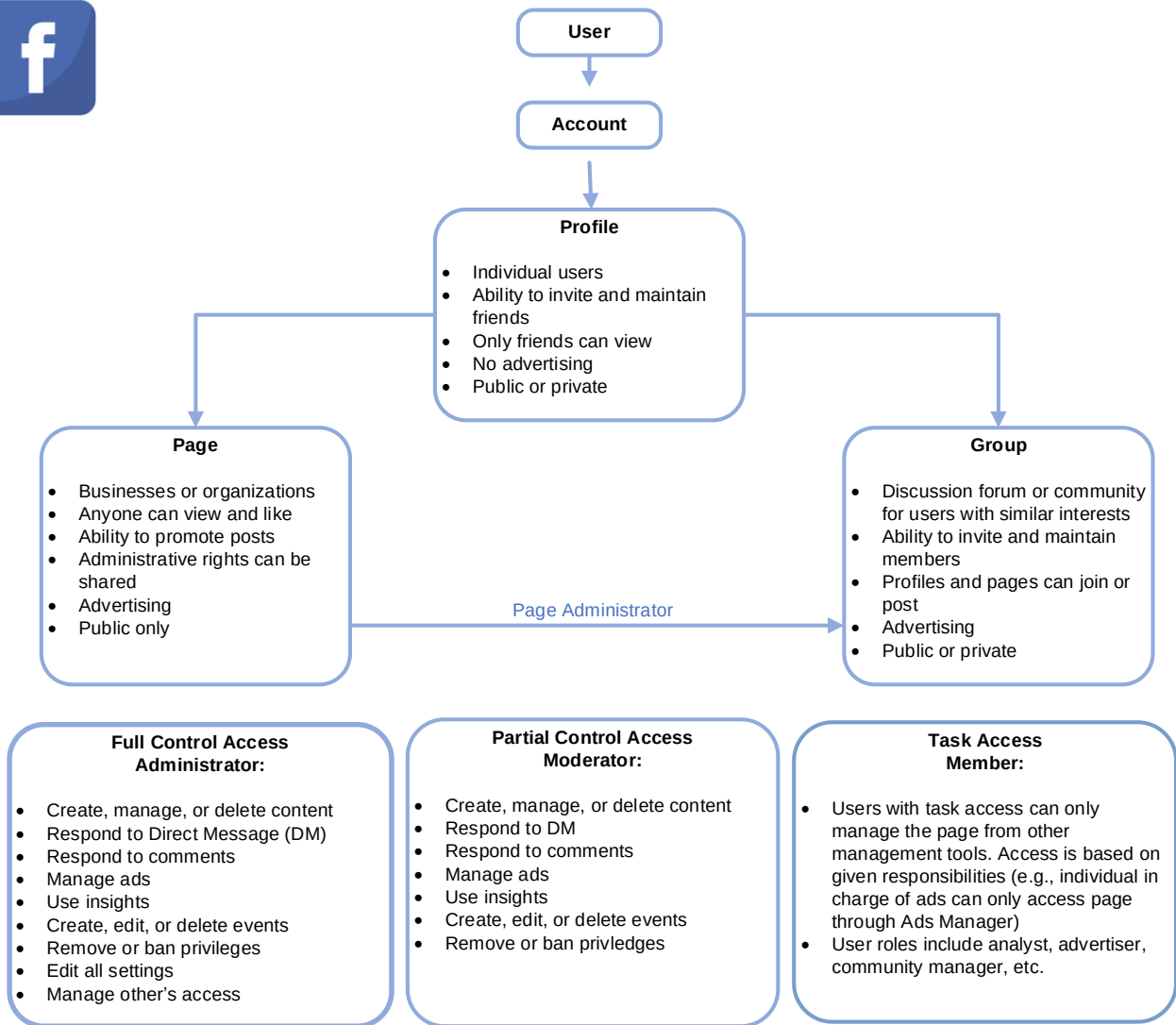
The District's social media guidelines recommend that schools and departments create and maintain at least one account on either Facebook, X, or Instagram. Each of these platforms require a primary account to be established using an active email address. Administrative capabilities vary depending on the platform and functions within the platform. Campus and department accounts are administered by various staff at the campuses or within the department who volunteer to manage these accounts.

³ Twitter changed to X in July of 2023. Auditors reviewed the controls in place surrounding Twitter.

⁴ According to the District's social media guidelines, it is recommended that schools create and maintain at least one account on Facebook, Instagram, or X. YouTube is not included in their guidance, so OIA decided to remove it from the scope of this audit.

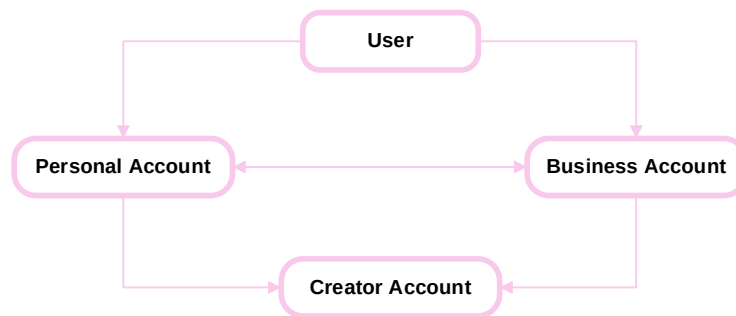
Facebook

Campuses often create Facebook pages to share information relevant to their school and its associated activities. Additionally, campuses often create groups for individual classes and various organizations within the campuses (i.e., first grade class, band, theater, etc.). To create a page or group, users are first required to have a personal profile and then multiple pages or groups can be created and managed under one Facebook account. Once a page or group is established, profile owners can assign full, partial, and task control access to others to manage the associated pages or groups; however, administrative rights cannot be given to manage the individual's personal profile.



Instagram

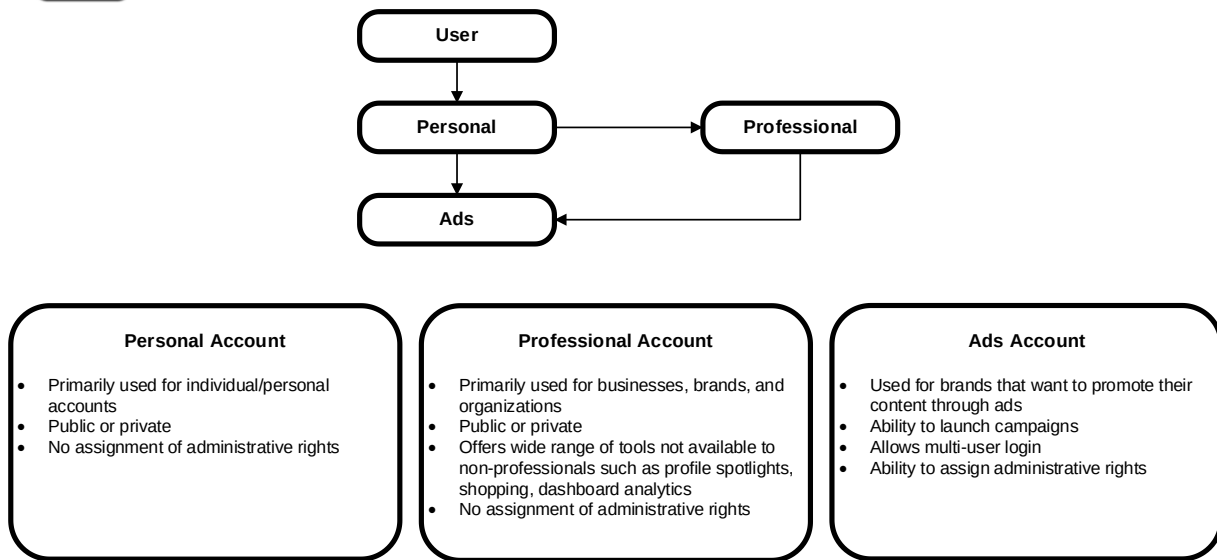
There are three types of Instagram accounts available: personal, business, and creator. Users can create personal or business accounts, but a creator account can only be established from a personal or business account. The administrative rights of business and creator accounts are similar as those mentioned for Facebook.



Personal Account	Business Account	Creator Account
<ul style="list-style-type: none">• Primarily used for individual/personal accounts• Public or private• No assignment of administrative rights	<ul style="list-style-type: none">• Primarily used for businesses/organizations• Public only• Access to analytics• Ability to add contact information• Allows for better DM management• Third-party app integration• Ability to assign administrative rights	<ul style="list-style-type: none">• Primarily used for public figures• Public only• Access to analytics• Ability to add contact information• Allows for better DM management• Ability to assign administrative rights

X

Three types of accounts are available for X users: personal, professional, and ads. Only one account can be established per email address. To have a professional or an ad account, a personal account must first be created.



Security/Privacy Settings

Privacy and security settings vary depending on the platform and the type of account. Primary privacy settings across platforms consist of the following:

- Viewing privileges – Who can see your account and the content posted
- Posting privileges – Who can post content and how the content is able to be posted
- Content sharing – Who and how your content can be shared

Other setting options include location tracking, notifications, comment filters, and direct messaging. Some of the primary privacy issues to be aware of regarding social media consist of:

- Data mining for identity theft
- Location tracking
- Harassment and cyberbullying
- Malware and viruses

In order to mitigate the above issues, it is important to ensure privacy settings are properly configured on social media accounts.

Social Media Strategy

Social media is an excellent free tool that the District can utilize to quickly connect and communicate with members of the community and also aide in promoting the organization. In order to make the best use of these free tools, it is important that an effective strategy be developed. Developing a social media strategy that outlines goals as well as key performance indicators (KPIs) helps an entity increase the effectiveness of its social media accounts.

Reach, engagement, and conversion are common social media KPIs that are used to measure performance and determine if connection with target audience is met. Social media platforms often provide data, typically referred to as analytics, that show stats on KPIs. Tracking metrics such as these allows the District to have insight into if the social media strategy is effective. Communication Services has established social media strategies for official district accounts to measure not only the engagement per platform, but the department also measures performance of individual campaigns.

Content Management

Content creation is a primary way for users to enhance social media engagement with its targeted audience. For the District's official social media accounts, posts are pre-planned, and the content is typically written by a coordinator in Communication Services and approved by the Communications director. Additionally, Communication Services has recently started to provide some pre-written content to campuses to improve uniform branding; however, most of the content development and management for campus accounts are created at the individual campuses.

Web Services

The Web Services Department within Communication Services manages the District's official website including website design, organization, and content creation. Similar to social media management, the campuses manage their individual sites with support from Web Services. Web Services provides regular training classes for campuses and departments and employees are then permitted to edit their department websites after registering and attending the website design training.

Scope

The audit focused on social media and web services processes for fiscal year (FY) 2022-2023.

Objective

The objective of the audit was to review the processes surrounding District affiliated social media accounts and web services to determine if controls are in place to properly manage social and web accounts effectively.

Methodology

OIA reviewed processes, controls, and supporting documents related to social media and web services. Auditors interviewed key personnel, conducted walkthroughs, and performed the following:

1. Account Administration – To determine whether adequate administrative oversight over social media exists, auditors performed the following:
 - Auditors requested an inventory of District affiliated social media accounts and associated administrators to determine if the information is accurate and properly maintained.
 - Auditors requested the District's social media guidelines to determine if account setup and account maintenance procedures are in place and sufficiently documented.
 - Auditors performed a walkthrough of social media account setup with Communication Services for Facebook, Instagram, and Twitter⁵. Additionally, auditors conducted background research and reviewed processes involving controls related to social media account review, termination, and tracking.

See Recommendation 1 in this report.

2. Account Security – To determine if controls are in place to properly secure District affiliated social media accounts along with any associated content, auditors conducted the following:
 - Auditors reviewed the privacy setting options for different platforms.
 - Auditors reviewed the District's processes surrounding social media account hacking prevention and detection and obtained and reviewed the crisis management plan.

See Recommendation 2 in this report.

2. Content Management - Auditors reviewed processes surrounding District affiliated social media content management. Additionally, auditors conducted searches for a random sample of campus Facebook Pages and reviewed posted content.
See Recommendations 3 and 4 in this report.

3. Strategy and Outreach – To determine whether the District has developed a comprehensive social media strategy that aligns with its stated mission, goals, and objectives and is regularly monitored to evaluate effectiveness, auditors obtained the departmental performance goals and reviewed processes surrounding social media account performance and messaging.
No observations were noted.

4. Website Management – To determine whether processes are in place to effectively and efficiently manage districtwide, campus, and department websites, auditors performed the following:
 - Reviewed Web Services' process surrounding website setup, content, and security.

⁵ Twitter changed to X in July of 2023. Auditors reviewed the controls in place surrounding Twitter.

- Randomly selected a sample of 30 campuses and reviewed their websites for the required content including general campus information, campus contact information, picture of the principal, and vertical team information.

No observations were noted; however, results were communicated to management for review.

Primary criteria used for this audit were:

- 1) Information Systems Audit and Control Association (ISACA) – How Do Organizations Control Their Use of Social Media? ISACA Journal Vol 2, Issued August 25, 2021
- 2) The Institute of Internal Auditors, Auditing Social Media – Adding Value by Improving Governance, Issued October 1, 2019

Audit Observations and Recommendations

Observation 1 – Processes, procedures, and controls surrounding authorization, administration, and management of District affiliated social media accounts could be enhanced.

Condition

Auditors reviewed processes for authorizing, administering, and managing District affiliated social media accounts and noted the following:

1. Account authorization

Campuses have the autonomy to set up their own District affiliated social media accounts, groups, pages, etc. without any approvals or authorizations. Communication Services encourages campuses to meet with them prior to creating a social media account; however, at the start of this audit, an official approval process had not been implemented to properly authorize District affiliated social media accounts. When creating a District affiliated social media account, Communication Services is now requiring departments and campuses to provide contact information of all administrators for that account.

2. Account administration

District affiliated social media accounts are typically established using the creators' personal email accounts. For example, Facebook requires business pages to be linked to personal accounts; and, as such, staff personal profiles are used to initiate and manage District affiliated accounts. These individuals are then responsible for assigning any additional administrators to the associated District affiliated accounts, pages, etc. if assistance is needed in managing the accounts.

The District's guidelines recommend that at least three campus or department employees (including the principal) have the password and access to prevent loss of access to an account in the event the account creator leaves the District. However, these guidelines do not currently cover the different types of administrative access and associated roles and privileges offered on the platforms nor do they cover best practices in assigning administrative access depending on the type of account and information being shared. For example, Facebook offers different levels of administrator access for groups and pages. Where viable, it may provide for greater controls to assign different types of administrators rather than sharing passwords.

3. Determining account type

Facebook and Instagram have different types of accounts that can be utilized depending on the purpose of the account as well as what types of functionalities are needed to manage the account. Auditors noted Communication Services has provided guidance on how to set up an account on the different platforms; however, no guidelines have been given for when to utilize which type of account under each platform. For example, campuses have the autonomy to choose a business or personal account when setting up an Instagram account even though a business account may be a better option in situations where greater controls or functions such as assigning administrative rights are needed.

4. Ending and transferring accounts

In the event a District affiliated social media account administrator leaves the District, there are no clear processes established for deactivating the account or removing and/or transferring rights. Per Communication Services, it is the responsibility of the campus to reach out to the department to notify them when an employee will no longer serve as an administrator on the account; however, there do not appear to be processes in place to effectively monitor this is occurring or to ensure the account was properly transitioned to a new administrator.

5. Maintaining an inventory of District affiliated social accounts and associated administrators

The Communication Services Department has created an inventory of District affiliated social media accounts; however, the list is not properly maintained to reflect current accounts and staff who are serving as administrators or who have access to the accounts. Per review of the inventory spreadsheet, there are 240 schools listed.

Cause

The extensive number of campuses and their District affiliated social media accounts makes it difficult to implement effective and efficient methods for proper oversight of District affiliated social media accounts. Campus staff that are tasked with managing social accounts are not compensated for these added responsibilities. Additionally, social media platforms are ever-changing with regard to their form, function, and controls, creating additional challenges.

Effect

Lack of documented guidelines, processes, and procedures for District affiliated social media accounts could lead to increased reputational, compliance, and/or legal risks for the District stemming from the following:

- Without proper controls surrounding account creation and administration, access to social accounts and associated content may not be properly restricted resulting in unauthorized access to private or sensitive information or unauthorized content being posted or shared on District affiliated accounts.
- The requirement for District affiliated social media accounts to be established using personal email accounts and profiles could result in the District losing control over the account and the associated content if the owner separates from the District. This may result in the inability to obtain information subject to public information requests. Lack of guidelines and controls to mitigate these risks may increase the potential for District affiliated social media accounts to

be compromised or lost.

- Finally, lack of a comprehensive inventory of District affiliated social media accounts makes it difficult for the appropriate owner to monitor accounts, administrators, access, and associated content.

Recommendation 1

To provide more effective management and oversight of District affiliated social media accounts, Communication Services should consider further developing detailed guidelines, processes, and procedures surrounding the below activities:

1. Authorizing District affiliated social media accounts – Policies, processes, and procedures should be enhanced for authorizing District affiliated social media accounts, profiles, pages, etc. A workflow could be developed for requesting, reviewing, and approving accounts prior to setup. It is recommended that the review and approval process be properly documented.
2. Account administration – Guidelines should be established for properly assigning account administrators and associated access.
 - Guidelines should implement best practices and controls when providing access to District affiliated social media accounts. Guidelines should cover the different types of administrator options, their associated access and privileges, and when each type should be utilized based on the type/purpose of the account and information shared (i.e., Facebook administrators that are given full, partial, and/or task access for groups/pages).
 - Where possible, a Communication Services administrator should have full control over any District affiliated social media accounts. For instances Where personal email accounts are utilized, guidelines and training should be established for mitigating risks of compromise.
 - Additionally, Communication Services should consider requiring training for account administrators on how to properly manage District affiliated social media accounts.
3. Determining account type – Guidelines should be established for when to use which type of account for the various platforms. Guidelines should be based on which type of account (i.e., group, page, business, creator) would be best given the purpose the account is intending to serve as well as which types of accounts will allow for the best controls for managing the account and associated content.
4. Ending and transferring accounts – Guidelines should be established to provide instructions for when an account needs to be deactivated or transferred. Where applicable, workflows could be established so that the changes in administrative duties are documented and can be easily tracked and managed. Guidelines should take into consideration, but not be limited to the following:
 - Record retention
 - Communication of the account changes to applicable parties

- Transfer of administrator rights
 - Resetting of passwords
5. Maintaining an inventory of District affiliated social accounts and associated administrators – Communication Services could use the workflow recommended in number one above to properly document and maintain an inventory of District affiliated social media accounts. The inventory listing should consist of the following:
- Listing of platforms, accounts, pages, etc. associated to each campus/department
 - Names of administrators and others who have access or roles
 - The email utilized to create the account (preferably centrally established and managed)
 - Passwords to accounts (password manager)

Additionally, where viable, Communications Services should consider determining all previously established active District affiliated social media accounts along with the associated administrator so they can be properly documented on the inventory listing.

Criteria

Information Systems Audit and Control Association (ISACA) – How Do Organizations Control Their Use of Social Media? ISACA Journal Vol 2, Issued August 25, 2021

How an organization manages its social media is crucial and starts with adequate account management and prevention of hacking and hijacking. There should be a documented handover process in the event an employee leaves the organization, that should include the process for password changes.

Organizations that utilize social media should have a mechanism to identify and register social media channels and a comprehensive list of employees and third parties responsible for those channels. Additionally, complex and varied passwords should be required for all online accounts and all official social media accounts should be linked to a generic enterprise email address.

Risk Level for Observation 1: High⁶

⁶ See Attachment 1 for Definition of Risk Level.

Observation 2 – Rules and requirements for configuring District affiliated social media account security/privacy settings should be implemented.

Condition

Auditors reviewed available account security controls for the different social media platforms the District utilizes and then reviewed the District's processes for properly securing its social media accounts noting a lack of the following controls surrounding District affiliated social media accounts:

1. Security/privacy controls

Communication Services has not established sufficient guidelines for properly securing District affiliated social media accounts and associated content. No guidance is in place for enabling applicable security and privacy settings on District affiliated social media accounts to provide for the safest online environment. The Department has provided some general instructions for how to set up a Facebook, Instagram, and X account; however, these instructions do not provide security/privacy setting configuration suggestions or requirements.

No guidance has been given related to when an account, page, group, etc. should/can be public or private, what measures should be taken when accepting followers, members, etc. or when followers/members should or should not be allowed to post.

For example, Facebook groups are often established at campuses for student organizations or for individual grade levels (i.e., a group created for all first-grade classes at a particular elementary school) where student pictures and other privileged information is posted. Auditors noted procedures have not been developed for verifying followers are appropriate considering the potentially private nature of the posted content that is shared with the group or page.

2. Password management controls

Password management controls have not been formally established for District affiliated social media accounts. Some platforms only allow for a single administrative user, so passwords must be shared amongst campus personnel. There are insufficient procedures in place for updating passwords on a regular basis, when an account becomes compromised, or when an employee with access to the account separates from the District or no longer needs access to the account.

3. Other high-risk areas where privacy settings are available but guidance, recommendations, or procedures for implementing these settings have not yet been developed are:

- Location tracking – potential for the location of students to be disclosed
- Data sharing – potential for district, employee, and/or student data to be compromised
- Direct messaging – potential for malware and viruses to be sent via direct messages
- Sharing rights – if a user shares something with a friend/follower and they repost it, the friend's friends can also see the information. The original user's reposted information is now in front of a completely different audience.

Cause

Security and privacy threats are constantly appearing within the social media environment; and, as such, proper security and privacy measures can be difficult to manage especially when utilizing a decentralized strategy. Additionally, security/privacy measures vary by platform and change frequently making it challenging to stay up to date on security configurations.

Effect

1. Security/privacy controls – insufficient procedures surrounding configuration and monitoring of account security and privacy settings could result in District affiliated social media accounts not adhering to local, state, or federal policies such as student privacy regulations.
2. Password management controls – lack of proper password controls could allow for unauthorized access to District affiliated social media accounts and associated content.

Recommendation 2

In order to better secure District affiliated social media accounts to provide for a safer online social environment, Communication Services should consider implementing the following controls:

1. Security/privacy controls – Communication Services should develop guidelines and/or requirements for configuring District affiliated social media account settings for the different platforms utilized. Guidelines should cover, but not be limited to, the following settings, where applicable:
 - Public vs private
 - Posting rights
 - Follower/friend/member request acceptance (use of verification questions should be considered where appropriate)
 - Follower privileges and rights
 - Content sharing
 - Removing followers/friends
 - Location tracking
 - Direct messaging
 - Data sharing

Communication Services should also consider implementing processes to monitor higher-risk District affiliated social media accounts are configured with the proper security settings.

2. Password management controls – Communication Services should formally establish password management guidance for District affiliated social media accounts. Guidance will need to consider that passwords often have to be shared as some platforms only allow for a single administrator.
3. Additional security risks – Communication Services should establish processes, procedures, and/or guidelines for the following:

- Access to District affiliated social media accounts via personal devices
- Account hacking prevention and detection
- Crisis management as related to social media

Criteria

Information Systems Audit and Control Association (ISACA) – How Do Organizations Control Their Use of Social Media? ISACA Journal Vol 2, Issued August 25, 2021

How an organization manages its social media is crucial and starts with adequate account management and prevention of hacking and hijacking. Often, sites are not updated regularly, users do not log out after each session, users share social media credentials with other team members and users willingly connecting with unknown parties.

There should be a documented handover process in the event an employee leaves the organization, that should include the process for password changes.

Information Systems Audit and Control Association (ISACA) – How Do Organizations Control Their Use of Social Media? ISACA Journal Vol 2, Issued August 25, 2021

The management of social media sites also requires attention to passwords and access. It should be determined whether access is controlled through limited permissions, in other words, is someone allowed to develop the content and others post the content. Additionally, complex and varied passwords should be required for all online accounts and all official social media accounts should be linked to a generic enterprise email address.

Risk Level for Observation 2: High⁷

Observation 3 – Guidelines for managing District affiliated social media content should be enhanced.

Condition

Auditors reviewed the District's social media policies, processes, and procedures surrounding management of content posted to District affiliated social media accounts noting there are currently no sufficient policies or guidelines established for determining appropriate content.

Campuses are primarily responsible for determining, posting, and managing content on their District affiliated social media accounts. There is currently insufficient guidance developed to assist campuses in establishing appropriate content for District affiliated social media accounts to ensure content complies with any applicable laws and regulations, content is aligned with District messaging, content encourages engagement, etc.

Additionally, no guidelines have been given for managing content posted by followers, friends, members, etc. when applicable.

⁷ See Attachment 1 for Definition of Risk Level.

Cause

Given the extensive number of District affiliated accounts along with their varying interests, it is exceedingly difficult to determine effective and efficient methods for content development.

Effect

Insufficient guidance for managing social media content could result in ineffective, inappropriate, and/or uncoordinated messaging, resulting in reputational risks as well as missed opportunities for enhancing connections with stakeholders.

Additionally, lack of guidelines to assist campuses in properly managing social media content could lead to increased risk of District social platforms being used for harassment and bullying.

Recommendation 3

To ensure content on District affiliated social media accounts is appropriate and aligned with District messaging, Communication Services should develop guidelines, processes, and procedures for campuses to use to properly manage District affiliated social media content. Below are some potential strategies to consider:

1. Develop a code of conduct for District posted content.
 - Consider requiring administrators or content creators to sign off on the code of conduct.
2. Develop a code of conduct for followers, members, etc. with posting/comment rights.
 - Consider utilizing account settings for the following where applicable:
 - Settings that require followers, members, etc. to agree to the code of conduct prior to the administrator accepting the request
 - Settings that allow the administrator to review and approve the content or comment prior to posting
3. Create a social media style guide that social accounts and content must adhere to.
4. Continue to establish universally relevant content that can be used across social accounts such as campus pages.
5. Develop guidelines that provide instructions for moderating comments and posts made by followers.
 - As noted in Observation 2, guidelines should first determine when it is appropriate to permit followers to post (for example, private groups may allow for posting rights, but public pages may limit these rights to administrators only). Guidelines should include information on what types of comments can/should be deleted.
6. Provide a method for any inappropriate social media content to be reported to Communication Services.
7. Provide training for account administrators on content creation.

Criteria

Information Systems Audit and Control Association (ISACA) – How Do Organizations Control Their Use of Social Media? ISACA Journal Vol 2, Issued August 25, 2021

Organizations that utilize social media should have a mechanism to identify and register social media channels and a comprehensive list of employees and third parties responsible for those channels. It should also be clear what sign-off procedures are for posting content. There must also be clearly defined style guidelines for content, including:

- Tone of voice, language, and key words
- Permissible content and areas of interest
- Rules for use of photography and branded imagery
- Rules for the use of competitions and promotional activities
- Posting schedule and content calendar
- Moderations of user-generated content

It should be determined whether access is controlled through limited permissions, in other words, is someone allowed to develop the content and others post the content. This refers to segregation of duties and prevents individuals from posting inappropriate or poorly developed statements prior to review and approval.

Information Systems Audit and Control Association (ISACA) – How Do Organizations Control Their Use of Social Media? ISACA Journal Vol 2, Issued August 25, 2021

It is recommended that organizations monitor all postings, ideally more than once a month. The organization should also have procedures in place to deal with false or dangerous postings. Clarity must be established regarding what can and cannot be posted, with an organizational policy that covers the following:

- Scope – Allow only certain channels and blogs
- Who – Permit only trained and authorized employees to post on social media channels
- Actions – Do not click on suspicious links
- Training – Provide training for new users and those who do not follow policy
- Reporting – Have a mechanism to report any inappropriate use of social media by employees, third parties or the public

Risk Level for Observation 3: High⁸

Observation 4 – District affiliated social media accounts should be easily identifiable, communicated, and promoted.

Condition

Auditors attempted to review District affiliated social media accounts across the different platforms noting searches would often bring up multiple accounts with various types of posts/information. It was difficult for auditors to differentiate between current and relevant District affiliated social media accounts and outdated accounts, spam accounts, and/or accounts created by unaffiliated individuals. For example, auditors did a Facebook page search for 5 random campus pages noting anywhere from 2-8 pages were populated for the search results.

Auditors also noted campus accounts typically did not contain any uniform branding that would make them identifiable as a valid District affiliated social media account.

⁸ See Attachment 1 for Definition of Risk Level.

Cause

Auditors found unofficial Facebook pages were often created as a result of a Facebook flaw that automatically creates pages when users check into places where the address is not linked to an established account. Although these pages will be listed as unofficial, it is still often unclear to the user which page is valid. In order to prevent this from occurring, Facebook advises that organizations claim their address on their relevant pages.

Other factors that may contribute to multiple, outdated, and/or spam accounts:

- High turnover of account administrators who often use personal email accounts to set up the campus social accounts. When turnover occurs, access to the accounts can be lost and new accounts must be created.
- Lack of processes, procedures, and training on how to avoid subjecting accounts to spam or hacking
- Lack of processes to identify and remove inactive or spam accounts
- Lack of controls surrounding the authorization of accounts

Additionally, as noted throughout the report, the decentralized nature of social media account administration, lack of sufficient guidelines, and the unincentivized responsibility of campus personnel to manage social media has allowed for social accounts to be created without consideration for appropriate branding and style.

Effect

Inability to distinguish District affiliated social media accounts may cause confusion to end users that utilize social media to get current and relevant information. Additionally, if search results provide multiple accounts and end users are not able to determine the correct and current account, it may result in users not following the relevant account allowing for a decrease in engagement.

Recommendation 4

In order to assist end-users in being able to properly identify and follow the current and relevant District affiliated social media accounts, Communication Services should consider the following:

1. Identifying and removing spam, inactive, and/or unauthorized accounts – Communication Services should implement processes to deactivate or remove unofficial accounts, where viable.

Additionally, Communication Services should establish processes to periodically conduct searches for inactive, unauthorized, and spam accounts and take available actions necessary to have them claimed/deactivated.

Where viable, Communication Services should consider verifying high traffic pages with Facebook to establish them as the authorized page for that campus.

2. Communicating and promoting District affiliated social media accounts - a directory of District affiliated social media accounts could be established, and links could be listed on the District's website for end-user reference. Additionally, procedures could be implemented to require campuses to post links to their social accounts on their website.
3. Establishing uniform branding across social media accounts – Communication Services should consider developing uniform branding requirements for account creators to follow in order to become a District affiliated social media account. Requirements for District affiliated social media account profiles could consist of elements such as the following:
 - Profile photos that are consistent with District imaging
 - Contain up-to-date contact information
 - Contain a clear relationship with the District in the page name and/or profile description/bio
 - Profile description that is relevant and appropriate to represent the District
 - Follows the District's official accounts
 - Includes a link to the District's website
 - Maintain an appropriate posting frequency (i.e., must post at least once a month)

Any determined requirements should be properly communicated and included in the District's branding and style guidelines.

Criteria

Information Systems Audit and Control Association (ISACA) – How Do Organizations Control Their Use of Social Media? ISACA Journal Vol 2, Issued August 25, 2021

Organizations can take steps to reassure end users that their social media site is valid and unofficial sites are identified:

- Social media platforms often allow the addition of a “verified” label to pages and, if they do, it should be used.
- The organizations main website should include information about and links to its presence on social media.
- It should be someone's responsibility to check social media for impersonation sites, including emerging, special interest or lesser-known social media sites.
- An automated tool or service to detect impersonation should be used.

Information Systems Audit and Control Association (ISACA) – How Do Organizations Control Their Use of Social Media? ISACA Journal Vol 2, Issued August 25, 2021

Organizations that utilize social media should have a mechanism to identify and register social media channels. There must also be clearly defined style guidelines for content, including:

- Tone of voice, language, and key words
- Permissible content and areas of interest
- Rules for use of photography and branded imagery
- Rules for the use of competitions and promotional activities

- Posting schedule and content calendar

Risk Level for Observation 4: Medium⁹

Conclusion

Utilizing social media as a business tool allows the District to stay connected to stakeholders and communicate quickly to large audiences. As District affiliated social media content may greatly impact the reputation of the District, it is crucial that effective social media governance is in place to reduce associated risks.

It can be extremely difficult to manage the multitude of social media accounts effectively and efficiently in a District this size. Implementation of the recommendations in this report could aid in improving the administration and security for District affiliated social media accounts in order to provide a safer online community and encourage engagement from students, parents, and other community members.

We would like to thank Communication Services for their cooperation and assistance with this audit.

The audit was conducted in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. Those standards require OIA to plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our observations and conclusions based on our audit objectives. OIA believes the evidence obtained provides a reasonable basis for our observations and conclusions based on our audit objectives.

Respectfully submitted,

Robert Rubel

Robert Rubel, MBA, CPA, CIA, CISA
Chief Internal Audit Officer

Cc: Pamela Lear, Ed.D., Deputy Superintendent, Chief of Staff and Racial Equity Officer
Libby Daniels, Chief Communications Officer
Robyn Harris, Deputy Chief, Communication Services
Anastasia Reed, Director I, Communication Services
Tiffany Huitt, Chief Schools Officer, School Leadership

Acknowledgments:

Eva Narten, CPA, CIA, CISA, Deputy Chief, Internal Audit
Shelly Kelly, CPA, Audit Director
Sam Willson, CFE, Audit Manager
Jonathan Bryant, MBA, CIA, CFE Auditor II
Claire Chen, CPA, Auditor II

⁹ See Attachment 1 for Definition of Risk Level.

Definition of Risk Level

Risk Level	Definition
High	<p>High probability of occurrence that would significantly impact District operations and have a significant financial or compliance risk.</p> <p>These observations are defined as an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of the District.</p>
Medium	<p>Risks are considered to be substantially undesirable and pose a moderate level of risk exposure to District operations. Without appropriate controls, the risk will happen on a consistent basis.</p>
Low	<p>The risks are considered to be undesirable and could moderately expose the District. Without appropriate controls, the risk will occur some of the time.</p>

Management Response

Communication Services will define, through a glossary of terms, how to properly delineate internal governance of social media sites versus accounts operating externally, which would remain outside of the district's oversight.

Official District Social Media Account

- The main social media accounts for the district and managed by Communication Services
- District Affiliated Social Media Account
- A campus, school or department social media account managed by a Dallas ISD team member.
 - Does not include groups such as PTA, PTO, alumni pages, fan pages or pages not managed by a Dallas ISD team member.

Observation 1 – Processes, procedures, and controls surrounding authorization, administration, and management of District affiliated social media accounts could be enhanced.

Acknowledgement of observation:

- ☒ Agree
☐ Disagree

Recommendation 1

To provide more effective management and oversight of District affiliated social media accounts, Communication Services should consider further developing detailed guidelines, processes, and procedures surrounding the below activities:

1. Authorizing District affiliated social media accounts – Policies, processes, and procedures should be enhanced for authorizing District affiliated social media accounts, profiles, pages, etc. A workflow could be developed for requesting, reviewing, and approving accounts prior to setup. It is recommended that the review and approval process be properly documented.
2. Account administration – Guidelines should be established for properly assigning account administrators and associated access.
 - Guidelines should implement best practices and controls when providing access to District affiliated social media accounts. Guidelines should cover the different types of administrator options, their associated access and privileges, and when each type should be utilized based on the type/purpose of the account and information shared (i.e., Facebook administrators that are given full, partial, and/or task access for groups/pages).
 - Where possible, a Communication Services administrator should have full control over any District affiliated social media accounts. For instances where personal email accounts are utilized, guidelines and training should be established for mitigating risks of compromise.

- Additionally, Communication Services should consider requiring training for account administrators on how to properly manage District affiliated social media accounts.
3. Determining account type – Guidelines should be established for when to use which type of account for the various platforms. Guidelines should be based on which type of account (i.e., group, page, business, creator) would be best given the purpose the account is intending to serve as well as which types of accounts will allow for the best controls for managing the account and associated content.
 4. Ending and transferring accounts – Guidelines should be established to provide instructions for when an account needs to be deactivated or transferred. Where applicable, workflows could be established so that the changes in administrative duties are documented and can be easily tracked and managed. Guidelines should take into consideration, but not be limited to the following:
 - Record retention
 - Communication of the account changes to applicable parties
 - Transfer of administrator rights
 - Resetting of passwords
 5. Maintaining an inventory of District affiliated social accounts and associated administrators – Communication Services could use the workflow recommended in number one above to properly document and maintain an inventory of District affiliated social media accounts. The inventory listing should consist of the following:
 - Listing of platforms, accounts, pages, etc. associated to each campus/department
 - Names of administrators and others who have access or roles
 - The email utilized to create the account (preferably centrally established and managed)
 - Passwords to accounts (password manager)

Additionally, where viable, Communications Services should consider determining all previously established active District affiliated social media accounts along with the associated administrator so they can be properly documented on the inventory listing.

Management's Response:

The audit's recommendation calls for enhanced policies, processes, and procedures for authorizing District affiliated accounts. Communication Services does not authorize or approve accounts for a campus, school, or department. Accounts are approved through department leadership or principal. To enhance record retention, Communication Services will request contact information for team members managing District affiliated accounts to better ensure access controls.

The recommendation includes establishing guidelines for assigning account administrators and access. This recommendation is not plausible as it only applies to Facebook pages. Communication Services will update the existing social media guidelines to include recommendations to team members when they are assigning access to a Facebook page.

Communication Services serves as the administrator for all official district social accounts and platforms. Due to the department's capacity, it is not reasonable for Communication Services to serve as administrators of all district affiliated social media accounts, which could include more than 240 school accounts per platform, hundreds of subject/level pages, along with departmental accounts. Furthermore, assigning ownership to a communications team member could limit our ability to post to the district's main account if an affiliated account becomes compromised. Communication Services provides social media guidelines and training for the appropriate social media account owners and managers (principals and department heads) to follow and govern accordingly.

The audit's recommendation calls for the development of social media guidelines, which Communication Services already has established and posted encompassing the most up-to-date tips and best practices for maintaining an impactful social media presence. However, the department recognizes the need to further enhance the existing social media guidelines by incorporating "account types", specific to campus and department accounts.

Communication Services cannot end a social media account; however, to align with District guidelines, each affiliated account must have at least three account holders for team members managing one. This will help ensure accounts are properly transferred should a team member no longer be responsible for managing a page. Semester based check-ins with principals and department heads will be established to maintain an up-to-date list of affiliated district social media accounts.

Estimated Implementation Date: January 2024

Communication Services will begin requesting account contact information for District affiliated accounts at the beginning of January 2024. This will occur twice a year. The department will also continuously update the social media guidelines to reflect the latest trends and best practices.

Individuals responsible for implementation:

Robyn Harris – Deputy Chief – Communication Services

Anastasia Reed-Jones – Director of Digital – Communication Services

Observation 2 – Rules and requirements for configuring District affiliated social media account security/privacy settings should be implemented.

Acknowledgement of observation:

☒ Agree

☐ Disagree

Recommendation 2

In order to better secure District affiliated social media accounts to provide for a safer online social environment, Communication Services should consider implementing the following controls:

1. Security/privacy controls – Communication Services should develop guidelines and/or

requirements for configuring District affiliated social media account settings for the different platforms utilized. Guidelines should cover, but not be limited to, the following settings, where applicable:

- Public vs private
- Posting rights
- Follower/friend/member request acceptance (use of verification questions should be considered where appropriate)
- Follower privileges and rights
- Content sharing
- Removing followers/friends
- Location tracking
- Direct messaging
- Data sharing

Communication Services should also consider implementing processes to monitor higher-risk District affiliated social media accounts are configured with the proper security settings.

2. Password management controls – Communication Services should formally establish password management guidance for District affiliated social media accounts. Guidance will need to consider that passwords often have to be shared as some platforms only allow for a single administrator.
3. Additional security risks – Communication Services should establish processes, procedures, and/or guidelines for the following:
 - Access to District affiliated social media accounts via personal devices
 - Account hacking prevention and detection
 - Crisis management as related to social media

Management's Response:

Communication Services is unable to control password requirements as that function is governed by the individual platform. The team will encourage the use of two-factor authentication for password management controls on district affiliated social media accounts, where applicable. We will encourage users to follow the minimum requirements to align with Dallas ISD's Educational Technology established protocols for district passwords.

The recommendation asks Communication Services to establish a process regarding the usage of personal devices to manage a district affiliated social media account. The use of electronic communication is governed through the [Technology Resources policy](#).

Estimated Implementation Date: January 2024

Individuals responsible for implementation:

Robyn Harris – Deputy Chief – Communication Services

Anastasia Reed-Jones – Director of Digital – Communication Services

Observation 3 – Guidelines for managing District affiliated social media content should be enhanced.

Acknowledgement of observation:

- ☒ Agree
☐ Disagree

Recommendation 3

To ensure content on District affiliated social media accounts is appropriate and aligned with District messaging, Communication Services should develop guidelines, processes, and procedures for campuses to use to properly manage District affiliated social media content. Below are some potential strategies to consider:

1. Develop a code of conduct for District posted content.
 - Consider requiring administrators or content creators to sign off on the code of conduct.
2. Develop a code of conduct for followers, members, etc. with posting/comment rights.
 - Consider utilizing account settings for the following where applicable:
 - Settings that require followers, members, etc. to agree to the code of conduct prior to the administrator accepting the request
 - Settings that allow the administrator to review and approve the content or comment prior to posting
3. Create a social media style guide that social accounts and content must adhere to.
4. Continue to establish universally relevant content that can be used across social accounts such as campus pages.
5. Develop guidelines that provide instructions for moderating comments and posts made by followers.
 - As noted in Observation 2, guidelines should first determine when it is appropriate to permit followers to post (for example, private groups may allow for posting rights, but public pages may limit these rights to administrators only). Guidelines should include information on what types of comments can/should be deleted.
6. Provide a method for any inappropriate social media content to be reported to Communication Services.
 - Provide training for account administrators on content creation.

Management's Response:

While the district's Employee Standards of Conduct applies to all district staff at all times, specifically here for electronic communications, Communication Services will update the existing social media guidelines to incorporate style guide recommendations for content. The guidelines will incorporate the following recommendations for district affiliated accounts to follow: naming conventions, profile image, profile biography, posting frequency, and social media best practices. The audit suggests the development of a code of conduct. These objectives are already achieved through the Employee Standards of Conduct. However, to better ensure team members are aware of proper social media etiquette, Communication Services will share tips and practices for

posting on the website. Communication Services will also add a statement to the district's website encouraging those who interact with district official and affiliated social media accounts to be respectful and adhere to the proper rules of social media engagement. This will be linked on the official social media accounts where applicable. While the audit recommends the creation of code of conduct for followers to adhere to, Communication Services has no control or purview over what someone posts on social media.

The recommendation suggests relevant content be provided for affiliated social accounts. Communication Services, through its Creative Services team, has always provided relevant content throughout the year for each campus to utilize through creative and marketing toolkits. The kits contain campaign social media graphics, banners, sliders, and content for campuses to post across multiple platforms. The information is shared with schools at the launch of each campaign and is district-aligned around relevant, universal messaging that each campus can easily share on their platforms.

<https://www.dallasisd.org/Page/76998>
<https://www.dallasisd.org/Page/86677>

While the audit recommends Hootsuite or similar platforms, which at times are effective, the tool comes with a sizable cost and limits the number of linked accounts it can service. Ultimately, the use of the tool has proven to be ineffective for the example provided. Communication Services recommends campuses and departments assess whether these platforms align with their current needs and resources.

Communication Services will update the existing social media guidelines to include tips and best practices for moderating Facebook groups and comments from followers.

While the current social media guidelines will be continuously updated to reflect the latest best practices for effective online presence, Communication Services has no governance of district affiliated accounts. While Communication Services currently conducts social listening to capture sentiments being shared about the district and better inform the department's social media strategy, we do not routinely and actively monitor District affiliated social media accounts.

Estimated Implementation Date: January 2024

Individuals responsible for implementation:

Robyn Harris – Deputy Chief – Communication Services

Anastasia Reed-Jones – Director of Digital – Communication Services

Observation 4 – District affiliated social media accounts should be easily identifiable, communicated, and promoted.

Acknowledgement of observation:

- ☒ Agree
☐ Disagree

Recommendation 4

In order to assist end-users in being able to properly identify and follow the current and relevant District affiliated social media accounts, Communication Services should consider the following:

1. Identifying and removing spam, inactive, and/or unauthorized accounts – Communication Services should implement processes to deactivate or remove unofficial accounts, where viable.

Additionally, Communication Services should establish processes to periodically conduct searches for inactive, unauthorized, and spam accounts and take available actions necessary to have them claimed/deactivated.

Where viable, Communication Services should consider verifying high traffic pages with Facebook to establish them as the authorized page for that campus.

2. Communicating and promoting District affiliated social media accounts - a directory of District affiliated social media accounts could be established, and links could be listed on the District's website for end-user reference. Additionally, procedures could be implemented to require campuses to post links to their social accounts on their website.
3. Establishing uniform branding across social media accounts – Communication Services should consider developing uniform branding requirements for account creators to follow in order to become a District affiliated social media account. Requirements for District affiliated social media account profiles could consist of elements such as the following:

- Profile photos that are consistent with District imaging
- Contain up-to-date contact information
- Contain a clear relationship with the District in the page name and/or profile description/bio
- Profile description that is relevant and appropriate to represent the District
- Follows the District's official accounts
- Includes a link to the District's website
- Maintain an appropriate posting frequency (i.e., must post at least once a month)

Any determined requirements should be properly communicated and included in the District's branding and style guidelines.

Management's Response:

Communication Services will maintain a directory of affiliated district social media accounts based on the semester check-ins with principals and departments.

Due to restrictions and limitations of social media platforms, Communication Services is unable to deactivate or claim unused accounts or remove unauthorized accounts. Where possible, Communication Services will report unauthorized or unused accounts through the social platform and will encourage those managing affiliated district social media accounts to do the same. This guidance will be provided through the social media guidelines.

The social media guidelines will address posting frequency, profile biography and profile photo requirements.

Estimated Implementation Date: March 2024

Individuals responsible for implementation:

Robyn Harris – Deputy Chief – Communication Services

Anastasia Reed-Jones – Director of Digital – Communication Services