International Journal of Research in Education Humanities and Commerce

Volume 07, Issue 05 "September - October 2026"

ISSN 2583-0333

CONFIDENTIALITY AS A PROFESSIONAL IMPERATIVE IN UNIVERSITY ADMINISTRATION: STAFF REACTIONS, ETHICAL TENSIONS, AND GOVERNANCE IMPLICATIONS: AN INTEGRATIVE REVIEW

OYETOLA, JULIANAH OLAWUMI
Registry Department
Ladoke Akintola University of Technology

YINUS S. O.
Department of Accounting, Faculty of Management Sciences
Ladoke Akintola University of Technology, Open and Distance Learning Centre, Oyo State

https://doi.org/10.37602/IJREHC.2026.7510

ABSTRACT

University administrative officers routinely manage sensitive personnel, academic, disciplinary, financial, and governance information, making confidentiality fundamental to professional integrity, institutional trust, and effective governance. However, confidentiality without timely and appropriate communication may be perceived by staff as secrecy, exclusion, or administrative opacity, thereby creating ethical tensions and weakening organizational trust. This study examines confidentiality practices, staff reactions, and their governance implications in university administration, with the aim of developing a balanced framework for ethical information management. A structured integrative review design (Evidence-synthesis method) was adopted, drawing on verified peer-reviewed empirical and conceptual studies, alongside relevant official regulatory and professional sources. The literature was identified through systematic searches of indexed bibliographic databases and reputable publisher platforms, with emphasis on studies published between 2018 and August 2026. Evidence was assessed for methodological transparency and relevance, extracted according to study design, context, evidence base, and principal findings, and synthesized thematically. Owing to heterogeneity in study designs, contexts, and outcome measures, statistical effect-size pooling was considered inappropriate; hence, narrative meta-synthesis was adopted. Findings indicate that effective confidentiality depends on formal information-governance systems, ethical leadership, supportive organisational culture, continuous role-specific training, and perceptions of procedural, interpersonal, and informational justice. The review further establishes that sustainable confidentiality requires protecting sensitive information while transparently communicating authorised procedures, decision rules, timelines, and outcomes. The study concludes that confidentiality should not constitute blanket secrecy but should operate within a socio-technical governance framework balancing need-to-know access, data protection, professional discretion, transparency, and accountability. It recommends clear policies, continuous training, authorised communication, ethical leadership, and bounded transparency to strengthen trust, administrative effectiveness, and good university governance.

Keywords: Confidentiality; University Administration; Information Governance; Staff Trust; Organisational Justice; Data Protection

Volume 07, Issue 05 "September - October 2026"

ISSN 2583-0333

1.0 INTRODUCTION

Universities are information-intensive organisations whose core functions of teaching, research, community engagement, personnel administration, and governance depend on the creation, movement, preservation, and authorised disclosure of records. Administrative units—particularly the Registry and allied human-resource, academic-affairs, examinations, legal, and governance offices—routinely handle information whose premature, inaccurate, or unauthorised disclosure may affect careers, academic progression, institutional reputation, due process, and personal dignity. In this environment, confidentiality is not simply a desirable personal trait; it is a professional and governance obligation that must be supported by policy, records systems, access controls, leadership, and ethical judgement.

The digitalisation of university administration has increased both the value and vulnerability of institutional information. Contemporary higher-education institutions operate open and complex information environments that combine staff and student databases, learning platforms, electronic records, cloud services, email, mobile devices, and distributed decision-making. A 2026 systematic review of information-security practices in higher education concluded that sustainable protection requires an integrated approach combining adaptive policy, continuous context-specific training, organisational culture, and technology rather than fragmented technical controls alone (Bwiino et al., 2026). Similarly, recent work on university security culture shows that higher-education institutions require security practices that are institution-wide, context-aware, and embedded in everyday work rather than treated as purely technical responsibilities (Albinali et al., 2025).

For Nigerian university administrators, confidentiality also exists within a changing legal and professional environment. The Nigeria Data Protection Act 2023 formalises obligations relating to lawful processing and protection of personal data, while the Public Service Rules provide a wider public-sector framework for official conduct and responsible handling of government information. Professional expectations are reinforced by the Association of Nigerian University Professional Administrators (ANUPA), whose current code of conduct and strategic values emphasise integrity, transparency, responsibility, accountability, equity, fairness, efficiency, and professionalism. The important implication is that confidentiality and transparency should not be treated as opposites; rather, they must be balanced within lawful and ethically defensible information governance.

The central challenge is therefore relational as well as technical. Staff members may respect an administrative officer who is discreet, fair, and dependable, yet the same refusal to disclose restricted information may provoke suspicion, frustration, social pressure, accusations of favouritism, or perceptions that management is concealing information. Evidence from higher education shows that organisational justice and trust shape employee attitudes, while information-security research consistently identifies communication, leadership commitment, awareness, and culture as determinants of compliant behaviour (Alshare et al., 2018; Paek & Lee, 2025; Snyman et al., 2023). This article repositions confidentiality from an individual "watchword" to an institutional professional imperative and examines the conditions under which it produces trust rather than distrust.

1.1 Statement of the Problem

Volume 07, Issue 05 "September - October 2026"

ISSN 2583-0333

University administrative officers occupy a difficult position at the intersection of information, authority, employee expectations, and institutional accountability. They may have advance access to promotion decisions, disciplinary proceedings, appointments, examination outcomes, committee deliberations, medical or legal reports, and other sensitive records. Ethical and legal obligations require them to prevent unauthorised disclosure, yet staff members directly affected by such information often seek explanations, reassurance, or early access. When communication channels are weak, delayed, inconsistent, or perceived as unfair, confidentiality may be reinterpreted as secrecy, bureaucratic arrogance, favouritism, or deliberate exclusion. This creates what may be described as a confidentiality–transparency paradox: the administrator must protect restricted content while simultaneously sustaining staff confidence in the fairness and legitimacy of institutional processes.

The original discourse on confidentiality in university administration has often been normative, emphasising the duty to keep official information secret. That approach is insufficient for contemporary universities because it does not adequately account for digital data governance, employee perceptions of justice, security culture, formal access control, or the need for timely authorised communication. Moreover, much of the literature specifically addressing Registry practice in African universities is dispersed across records management, information security, organisational behaviour, and public-administration research. A more integrated evidence base is needed to explain not only why confidentiality matters, but how it should be practised and communicated so that it strengthens rather than erodes trust. This study aim to assess confidentiality practices, staff reactions, and their governance implications in university administration, with a view to developing an effective governance framework.

1.2 Innovation of the Study

This review is significant at four levels. For university administrators, it provides a defensible approach to handling sensitive information without unnecessarily alienating staff. For university management, it identifies system-level requirements—policy, role-based access, communication protocols, staff training, auditability, and leadership modelling—that reduce dependence on individual discretion. For employees and unions, it clarifies why confidentiality may legitimately restrict access to content while still requiring fairness, explanation, and timely official communication. For scholarship, it connects records management and information-security evidence with organisational justice and trust, thereby extending discussion of confidentiality beyond the traditional language of secrecy and discretion.

2.0 LITERATURE REVIEW

2.1 University Administration and the Registry as an Information-Governance Hub

The Registry is central to institutional continuity because it supports statutory decision-making, preserves official records, coordinates personnel and academic processes, and provides documentary evidence of institutional action. In contemporary settings, this role extends beyond physical custody of files to information governance: defining who may access which data, for what purpose, under what authority, for how long, and through what secure channel. African higher-education research indicates that records management remains uneven and is often constrained by policy gaps, resource limitations, weak implementation tools, and organisational factors (Simwaka et al., 2023).

Volume 07, Issue 05 "September - October 2026"

ISSN 2583-0333

Empirical evidence from the University of Cape Coast illustrates why access control is fundamental. Andoh and Attafuah (2021) found that strategies for controlling access to human-resource records could protect security and confidentiality, although existing and anticipated challenges remained. This is directly relevant to university Registry practice: confidentiality is more reliable when it is institutionalised through access rules, record classification, custody arrangements, and traceable processes rather than left solely to the personal discretion or memory of individual officers.

2.2 Distinguishing Confidentiality, Privacy, Secrecy, Security, and Transparency

Confidentiality refers to the duty to prevent information entrusted for a legitimate purpose from being disclosed to unauthorised persons. Privacy concerns the rights and interests of individuals in relation to their personal information and private life. Information security is broader and includes the preservation of confidentiality, integrity, and availability of information through technical, organisational, and behavioural controls. Secrecy, by contrast, is a condition of non-disclosure and may or may not be justified. Transparency concerns openness about relevant processes, criteria, decisions, and accountability. These concepts overlap but are not interchangeable.

A professional administrative officer therefore does not fulfil confidentiality merely by refusing to speak. The officer must know whether information is restricted, who is authorised to receive it, whether disclosure is required by law or policy, how disclosure should occur, and what procedural information can appropriately be communicated. The distinction is important because excessive secrecy can generate the same mistrust that confidentiality is intended to prevent. Evidence on transparency and trust in public institutions suggests that disclosure practices can affect trust, while higher-education studies show that fairness and trust are closely linked to employees' perceptions of organisational processes (Ripamonti, 2024; Snyman et al., 2023).

2.3 Legal and Professional Framework in Nigeria

The Nigeria Data Protection Act 2023 provides the principal contemporary legal framework for personal data protection in Nigeria. For university administration, its relevance extends to personnel records, student records, disciplinary files, medical information, payroll data, contact details, identity information, and other data processed in the course of institutional duties. The practical implication is that access to personal data should be purpose-bound, lawful, proportionate, and secured against unauthorised use or disclosure (Federal Republic of Nigeria, 2023).

The Public Service Rules remain an important ethical and disciplinary reference for official conduct in Nigeria's public sector and reinforce the expectation that official information is handled responsibly. In parallel, ANUPA's professional code and strategic values emphasise integrity, transparency, responsibility, accountability, equity, fairness, efficiency, and effectiveness. These values are particularly useful because they show that professional university administration is not built on secrecy alone: confidential handling of information must coexist with transparent, fair, and accountable administrative processes (Association of Nigerian University Professional Administrators [ANUPA], n.d.; Office of the Head of the Civil Service of the Federation [OHCSF], 2021).

2.4 Theoretical and Conceptual Lens

This review draws primarily on organisational justice and socio-technical information-security perspectives. Organisational justice is particularly relevant because staff reactions to confidentiality are often reactions to how decisions are made, explained, and communicated. Procedural justice concerns the perceived fairness of decision procedures; interpersonal justice concerns dignity and respectful treatment; and informational justice concerns the adequacy and honesty of explanations. In a higher-education information-security case study, Alshare et al. (2018) found that procedural and distributive justice, privacy, responsibility, sanctions, and organisational security culture were significant predictors of information-security policy violations. Nigerian evidence also shows that justice perceptions are associated with workplace behaviour in public universities (Obalade & Mtembu, 2023).

The socio-technical security perspective treats secure behaviour as the product of interacting people, processes, culture, leadership, and technology. Recent evidence reviews show that management commitment, policy compliance, communication, training, monitoring, and broader organisational culture shape security behaviour (Bwiino et al., 2026; Sutton & Tompson, 2025). Applied to Registry work, this perspective implies that ethical confidentiality cannot be sustained by personal virtue alone. It requires institutional systems that make the correct behaviour clear, feasible, monitored, and culturally supported.

2.5 Empirical Evidence Synthesis

The evidence consistently indicates that confidentiality in modern organisations is not a single behaviour but an outcome of governance, culture, communication, awareness, fairness, and access control. Table 1 summarises selected studies that most directly informed the synthesis.

Table 1. Selected empirical and review evidence relevant to confidentiality in university administration

Study	Context/design	Sample/evidence base	Key finding	Relevance
Bwiino et al. (2026)	Systematic review; higher education information security	358 records identified; 41 studies included after screening	Sustainable security requires integrated policy, continuous context-specific training, organisational culture, and technology.	Supports a socio-technical rather than individual-discretion model of confidentiality.
Albinali et al. (2025)	Review/taxonomy of university security culture	University-focused formal and practice literature	Security culture in universities remains underdeveloped and requires institution-wide best practices.	Shows the need to embed confidentiality in university culture and governance.
Sutton & Tompson (2025)	Rapid evidence review of cybersecurity culture	1,768 records; 59 eligible studies	Management involvement, employee attitudes, policy compliance,	Explains why leadership and communication matter for

Study	Context/design	Sample/evidence base	Key finding	Relevance
			training, monitoring, and culture jointly shape behaviour.	confidential behaviour.
Paek & Lee (2025)	Online survey and structural equation modelling	Full-time employees in South Korea	Awareness strongly predicted vigilance; communication, commitment, feedback, and monitoring increased awareness.	Supports communication and feedback as complements to confidentiality controls.
Ramadhan et al. (2024)	Qualitative case study; Indonesian public universities	Public-university data-governance stakeholders	Internal and external institutional factors affect data-governance implementation.	Shows that confidentiality depends on governance structure, not only individual ethics.
Simwaka et al. (2023)	Hermeneutic review; African higher education	African higher-education records-management literature	Records management is practised but constrained by multiple organisational and resource factors; formal tools are needed.	Provides direct African evidence for stronger records-governance systems.
Snyman et al. (2023)	Cross-sectional survey; South African higher education institution	N = 493 academic and support staff	Organisational justice and trust functioned as positive mediating mechanisms in employee–organisation relations.	Supports the role of fairness and trust in staff reactions to administrative decisions.
Obalade & Mtembu (2023)	Quantitative survey; Nigerian public universities	N = 572 employees	Dimensions of organisational justice were associated with workplace deviance; interpersonal justice reduced organizational deviance.	Provides Nigerian evidence that treatment and fairness shape staff behaviour.
Amankwa et al. (2022)	Survey/PLS-SEM; Ghana	N = 313 employees in 10 organisations	Organisational and behavioural factors jointly shape information-security policy-compliance culture.	Shows that compliance is cultural and behavioural as well as procedural.
Andoh & Attafuah (2021)	Qualitative study; University of Cape Coast, Ghana	Human-resource staff; purposive sampling	Access-control strategies protected HR records, although challenges persisted.	Directly supports controlled access to sensitive

Study	Context/design	Sample/evidence base	Key finding	Relevance
				personnel information.
Khando et al. (2021)	Systematic literature review	Empirical information-security awareness literature	Technical controls alone are insufficient; awareness and human factors remain central.	Supports continuous staff education and role-specific security awareness.
Alshare et al. (2018)	Higher-education case study; regression analysis	N = 195 usable responses	Procedural/distributive justice, privacy, responsibility, sanctions, and security culture predicted policy violations.	Directly links fairness, privacy, culture, and compliance in higher education.

2.6 Literature Gap

Three important gaps justify the relevant of this study. First, recent higher-education information-security research has concentrated largely on cybersecurity policy, technological controls, awareness, and compliance, whereas the interpersonal consequences of administrative confidentiality—especially staff reactions to restricted information—remain comparatively underexamined (Albinali et al., 2025; Bwiino et al., 2026). Second, African research has documented persistent records-management and access-control challenges in higher education, but relatively little work integrates these operational issues with organisational justice, staff trust, and communication (Andoh & Attafuah, 2021; Simwaka et al., 2023). Third, Nigerian university research on organisational justice shows that staff behaviour is sensitive to how procedures and interpersonal treatment are perceived, yet this insight has not been sufficiently connected to confidentiality practice in Registry administration (Obalade & Mtembu, 2023).

The conceptual innovation of this paper is the proposed idea of bounded transparency. Bounded transparency means protecting the substantive content of information that is legitimately restricted while communicating, as fully as lawful and appropriate, the process, criteria, timelines, responsible authority, rights of review or appeal, and authorised final outcomes. The model rejects both indiscriminate disclosure and blanket secrecy. It frames confidentiality as a calibrated governance practice supported by procedural fairness, secure information architecture, role clarity, and professional communication.

3.0 METHODOLOGY

A structured integrative review design (Evidence-synthesis method) was adopted was adopted because the topic spans empirical studies, evidence reviews, legal instruments, professional standards, information-security research, records management, and organisational behaviour. Integrative reviews are suitable for synthesising heterogeneous evidence and generating conceptual understanding across methodological traditions (Snyder, 2019; Whittemore & Knafl, 2005). The approach was selected in preference to presenting the paper as a purely

conceptual essay because it allows the central arguments to be grounded in traceable and methodologically described evidence.

3.1 Search Strategy and Source Verification

The evidence base was updated through targeted searches completed to 18 August 2026. Searches were conducted across publisher and bibliographic platforms that included Elsevier/ScienceDirect, Wiley Online Library, Emerald, Springer Nature, PubMed/PMC, and indexed bibliographic records, together with official Nigerian government and professional websites. Search concepts were combined around the terms: university administration, registry, confidentiality, information security, information governance, data governance, records management, staff trust, organisational justice, policy compliance, higher education, Nigeria, and Africa. Recent sources published mainly from 2018 to 2026 were prioritised, while older methodological references were retained only where they were foundational to integrative-review methodology.

References were retained only when bibliographic details could be independently verified through a publisher, DOI record, recognised bibliographic database, or official institutional source. Older references in the source manuscript that could not be reliably verified were not carried forward. Official Nigerian sources were used for the Nigeria Data Protection Act, the Public Service Rules, and ANUPA's current professional ethics and strategic values.

3.2 Eligibility and Data Extraction

Sources were considered relevant when they met one or more of the following criteria:

- examined confidentiality, information security, data governance, access control, records management, organisational justice, employee trust, or policy compliance;
- focused directly on higher education or provided organisational evidence with clear relevance to university administrative practice;
- reported an empirical method, systematic/structured review method, or authoritative policy/regulatory framework; and
- provided sufficiently verifiable publication information to support accurate referencing.

4.0 RESULTS AND DISCUSSION: METAL ANALYSIS

Theme 1: Confidentiality Is a Governance System, Not Merely Personal Discretion

Across the evidence, the most consistent finding is that secure information handling depends on institutional governance. Andoh and Attafuah (2021) demonstrate the value of access controls for sensitive human-resource records, while Ramadhan et al. (2024) show that data-governance implementation is shaped by organisational structure and other internal and external conditions. African records-management evidence similarly indicates that formal policies and tools are required to sustain reliable practice (Simwaka et al., 2023).

For Registry administration, the implication is practical: confidential information should be classified; access should be role-based and purpose-specific; records should be stored in secure physical or digital environments; disclosures should be authorised and traceable; and

Volume 07, Issue 05 "September - October 2026"

ISSN 2583-0333

retention/disposal procedures should be defined. Confidentiality becomes vulnerable when staff rely on informal custody, shared passwords, unsecured messaging, uncontrolled printing, or ambiguous delegation.

Theme 2: Leadership and Organisational Culture Shape Confidential Behaviour

The second theme is that confidentiality is cultural. Sutton and Tompson (2025) found that cybersecurity culture depends on management involvement, employee attitudes, policy compliance, training, monitoring, and the wider organisational culture. Bwiino et al. (2026) reached a similar conclusion in the higher-education context, arguing that sustainable security requires integrated people, process, policy, and technology. Amankwa et al. (2022), working with employees in Ghana, also found that organisational and behavioural factors jointly influence information-security policy-compliance culture.

These findings suggest that administrative officers are more likely to maintain confidentiality when leaders model the same standards, policy breaches have predictable consequences, and secure behaviour is supported rather than undermined by informal requests from senior colleagues. A culture in which hierarchy can bypass rules weakens confidentiality even when junior officers are well trained.

Theme 3: Awareness, Communication, and Feedback Are Protective Controls

Security awareness is repeatedly associated with safer behaviour. Paek and Lee (2025) found awareness to be the strongest predictor of information-security vigilance, while communication, leadership commitment, feedback, and monitoring contributed to awareness. Khando et al. (2021) likewise concluded that technical controls alone cannot adequately protect information when human factors and awareness are neglected.

In university administration, this implies that confidentiality training should move beyond generic admonitions to ‘keep secrets’. Administrative officers need role-specific guidance on data classification, lawful bases for processing, authorised disclosure, secure email and messaging, password and device practices, meeting papers, minutes, personnel files, examination records, conflict of interest, and incident reporting. Staff outside the Registry also require orientation so that legitimate confidentiality is not misinterpreted as personal hostility.

Theme 4: Staff Reactions Are Filtered Through Justice and Trust

The evidence indicates that people respond not only to outcomes but also to how decisions are made and communicated. In a higher-education case study, Alshare et al. (2018) found that justice-related factors were significant predictors of information-security policy violations. Snyman et al. (2023) found that organisational justice and trust were important mechanisms in a South African higher-education workforce. In Nigerian public universities, Obalade and Mtembu (2023) demonstrated that justice dimensions were associated with employee deviance and that interpersonal justice could reduce organisational deviance.

Applied to confidentiality, these findings explain why two officers who withhold the same restricted information may provoke different reactions. An officer who communicates respectfully, explains the applicable process, gives realistic timelines, and applies the same rule

Volume 07, Issue 05 "September - October 2026"

ISSN 2583-0333

consistently is more likely to preserve trust than an officer who responds dismissively or selectively. Staff hostility may therefore reflect not only denial of information but perceived unfairness, unequal access, disrespect, or inadequate explanation.

Theme 5: Confidentiality and Transparency Are Complementary When Properly Bounded

The synthesis does not support a choice between confidentiality and transparency. Rather, effective governance requires both. ANUPA's current professional values explicitly include integrity, transparency, accountability, equity, and fairness, while Nigerian data-protection law requires responsible handling of personal information. Transparency about process can therefore coexist with confidentiality of content.

This review proposes bounded transparency as the most defensible practice model. Restricted substantive information—such as confidential deliberations, personal data, draft recommendations, protected investigations, or unauthorised results—remains protected. At the same time, the institution communicates what process is being followed, who has authority to decide, what criteria apply, when an official outcome is expected, how affected staff will be notified, and what review or appeal routes exist. This approach reduces the information vacuum in which rumour, suspicion, and pressure thrive.

Table 2. Proposed bounded-transparency framework for university administrative confidentiality

Domain	What remains confidential	What should be transparent	Expected governance effect
Personnel/promotion	Personal records, committee deliberations, unauthorised draft outcomes	Published criteria, timeline, responsible authority, authorised final communication, appeal process	Reduces rumours and perceptions of favouritism while protecting personal data
Disciplinary matters	Evidence, witness identities where protected, confidential panel deliberations	Due-process steps, rights of affected persons, timeline, official decision and review route	Protects dignity and fairness while preserving procedural legitimacy
Examinations/results	Unapproved results, examiner information where restricted, scripts/marking data as governed	Approval process, release schedule, correction/appeal procedure, authorised results	Protects academic integrity while reducing uncertainty
Council/Senate/management decisions	Confidential agenda papers and deliberations until authorized	Decision authority, implementation process, approved communiqués or circulars	Balances governance confidentiality with institutional accountability

Domain	What remains confidential	What should be transparent	Expected governance effect
Digital/personnel data	Credentials, personal identifiers, medical/financial data, access logs	Privacy notices, access rules, incident-reporting routes, data-subject procedures	Strengthens data protection and staff confidence

5.0 DISCUSSION OF FINDINGS

This review reframes confidentiality in university administration as a multidimensional governance practice. The traditional expectation that a good administrative officer should simply be discreet remains valid but incomplete. Contemporary evidence shows that secure information behaviour is produced by the interaction of policy, systems, training, management example, organisational culture, access control, fairness, and communication. The administrative officer remains morally accountable, but the institution also has a duty to design an environment in which confidential behaviour is clear, feasible, and consistently reinforced.The findings also clarify why staff reactions to confidentiality are mixed. Positive reactions—respect, confidence, willingness to entrust sensitive matters, and perceptions of professionalism—are more likely when staff believe that information is protected consistently and for legitimate reasons. Negative or ambivalent reactions—suspicion, pressure, hostility, labelling, or attempts to bypass the officer—are more likely when staff perceive unequal access, insufficient explanation, opaque procedures, or selective enforcement. Organisational justice provides a useful mechanism for understanding this pattern because employees judge both the outcome and the fairness of the process that produced it (Alshare et al., 2018; Obalade & Mtembu, 2023; Snyman et al., 2023).

The central practical lesson is that confidentiality should not become administrative silence. An officer may be unable to disclose a promotion outcome before formal approval, but can often explain the stage of the process, the authority responsible for approval, the expected mode of communication, and available procedures after release. Similarly, an officer may not disclose the details of a disciplinary investigation but can explain the applicable due-process steps and the rights of the affected person. Such communication does not weaken confidentiality; it strengthens legitimacy.

The digital environment increases the urgency of this distinction. Sensitive information now moves through email, shared drives, institutional platforms, mobile devices, cloud systems, video meetings, messaging applications, scanned documents, and portable storage. Each channel introduces access and disclosure risks. The 2026 higher-education review by Bwiino et al. underscores the need for system-wide integration of policy, training, culture, and technology. Universities should therefore combine professional ethics with technical and administrative safeguards such as least-privilege access, multi-factor authentication, secure document sharing, password management, audit logs, controlled printing, records classification, clean-desk practices, and incident-reporting procedures.

For Nigerian universities, the Nigeria Data Protection Act 2023 changes the conversation from optional discretion to demonstrable accountability for personal data. This legal environment should encourage Registry departments to collaborate with institutional data-protection

officers, ICT units, legal units, human resources, internal audit, and university management. Confidentiality is strongest when institutional responsibilities are distributed but coordinated, rather than placed entirely on the individual officer who happens to possess a file.

5.1 Practical Implications of the Study for University Administration

First, confidentiality policies should be written in operational language. Staff need to know categories of restricted information, authorisation pathways, permitted communication channels, escalation routes, and consequences of breaches. Second, universities should distinguish restricted content from information about process. This allows staff to receive legitimate explanations without compromising protected information. Third, administrators should be trained in tactful firmness: the ability to refuse unauthorised disclosure while remaining respectful, informative, and non-defensive. Fourth, communication delays should be treated as governance risks because prolonged information vacuums encourage informal networks, speculation, and pressure on administrative officers.

Finally, leadership modelling is indispensable. Where senior officials routinely request confidential information through unofficial channels or expect exceptions for themselves, formal confidentiality policies lose credibility. Conversely, when leaders use authorised channels and support officers who follow policy, secure behaviour becomes part of the institutional culture.

6.0 CONCLUSION AND RECOMMENDATIONS

Confidentiality remains a non-negotiable professional imperative in university administration, but its modern meaning extends beyond silence or secrecy. The evidence reviewed shows that confidentiality is sustained by information governance, access control, leadership, organisational culture, staff awareness, fairness, and communication. Administrative officers protect institutional integrity when they prevent unauthorised disclosure; they protect institutional trust when they do so consistently, respectfully, and within transparent procedures. The most defensible model is therefore bounded transparency: protect what must legitimately remain restricted, while communicating the process, authority, timeline, criteria, and authorised outcome as clearly as possible. When confidentiality and transparency are balanced in this manner, the Registry is more likely to be perceived not as a secretive bureaucracy but as a trustworthy custodian of institutional memory, due process, and professional integrity. Based on findings the following recommendations were made:

1. Universities should adopt a formal information-classification and confidentiality policy that identifies restricted information, authorised users, disclosure routes, retention requirements, and breach-response procedures. This is to establish confidential and non-retaliatory channels for reporting suspected breaches, coercion, unauthorised access, or misuse of institutional information.
2. Registry and allied administrative units should implement role-based and least-privilege access to both physical and electronic records, supported by secure storage, audit trails, and periodic access reviews.
3. Mandatory, recurrent training should be provided on confidentiality, the Nigeria Data Protection Act 2023, secure records handling, digital communication, social engineering, conflict of interest, and incident reporting.

4. Senior management should model compliance by using authorised channels and should protect administrative officers from improper pressure to release confidential information.
5. Registry, ICT, legal, human-resources, internal-audit, and data-protection functions should jointly conduct periodic information-governance audits and test the effectiveness of access controls and communication procedures.
6. Official communication systems, including institutional email, circulars, staff portals, and approved bulletins, should be strengthened so that staff do not depend on rumours or personal contacts for legitimate information.

REFERENCES

1. Albinali, M., Niazi, M., Alshayeb, M., Mahmood, S., & Khan, A. A. (2025). Taxonomy-based approach for understanding and enhancing security culture in universities. PeerJ Computer Science, 11, e3005. https://doi.org/10.7717/peerj-cs.3005
2. Alshare, K. A., Lane, P. L., & Lane, M. R. (2018). Information security policy compliance: A higher education case study. Information & Computer Security, 26(1), 91–108. https://doi.org/10.1108/ICS-09-2016-0073
3. Amankwa, E., Loock, M., & Kritzinger, E. (2022). The determinants of an information security policy compliance culture in organisations: The combined effects of organisational and behavioural factors. Information & Computer Security, 30(4), 583–614. https://doi.org/10.1108/ICS-10-2021-0169
4. Andoh, R. P. K., & Attafuah, A. (2021). Access control of human resource records: Case of the University of Cape Coast, Ghana. Collection and Curation, 41(1), 25–33. https://doi.org/10.1108/CC-06-2020-0025
5. Association of Nigerian University Professional Administrators. (edition 6). Ethics: ANUPA Nigeria code of conduct and strategic values. Retrieved August 18, 2026, from https://anupanigeria.com/ethics/
6. Bwiino, K., Mayoka, G. K., Nkamwesiga, L., & Nyamadi, M. (2026). A systematic literature review of information security practices in higher education contexts. IET Information Security, 2026(1), 1–19. https://doi.org/10.1049/ise2/6324508
7. Federal Republic of Nigeria. (2023). Nigeria Data Protection Act, 2023. Nigeria Data Protection Commission. https://ndpc.gov.ng/download/nigeria-data-protection-act-2023/
8. Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees' information security awareness in private and public organisations: A systematic literature review. Computers & Security, 106, 102267. https://doi.org/10.1016/j.cose.2021.102267
9. Obalade, G. O., & Mtembu, V. (2023). Effect of organisational justice on workplace deviance in Nigerian public universities. Acta Commercii, 23(1), a1091. https://doi.org/10.4102/ac.v23i1.1091
10. Office of the Head of the Civil Service of the Federation. (2021). Public Service Rules. The Presidency. https://ohcsf.gov.ng/publication/public-service-rules/
11. Paek, S. Y., & Lee, J. (2025). Promoting employees' information security vigilance by enhancing awareness: The roles of organizational climate and deterrence measures. Security Journal, 38, Article 12. https://doi.org/10.1057/s41284-024-00460-2

12. Ramadhan, A. F., Tajudeen, F. P., & Jaafar, N. I. (2024). The influence factors of data governance implementation: Study in Indonesian public university. Procedia Computer Science, 234, 1204–1211. https://doi.org/10.1016/j.procs.2024.03.116
13. Ripamonti, J. P. (2024). Does being informed about government transparency boost trust? Exploring an overlooked mechanism. Government Information Quarterly, 41(3), 101960. https://doi.org/10.1016/j.giq.2024.101960
14. Simwaka, K., Malanga, D. F., & Chipeta, G. (2023). Records management in institutions of higher education in Africa: A hermeneutic literature review. Global Knowledge, Memory and Communication, 74(5/6), 1400–1413. https://doi.org/10.1108/GKMC-02-2023-0070
15. Snyman, A. M., Coetzee, M., & Ferreira, N. (2023). The psychological contract and retention practices in the higher education context: The mediating role of organisational justice and trust. South African Journal of Psychology, 53(2), 185–198. https://doi.org/10.1177/00812463221129067
16. Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039
17. Sutton, A., & Tompson, L. (2025). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. Computers & Security, 148, 104110. https://doi.org/10.1016/j.cose.2024.104110
18. Whittemore, R., & Knafl, K. (2005). The integrative review: Updated methodology. Journal of Advanced Nursing, 52(5), 546–553. https://doi.org/10.1111/j.1365-2648.2005.03621.x

