Ethics, Data Privacy and Security: Pillars of a Modern Office Environment

[1]Sudetu OSENI and [2]Sophia V. ADEYEYE (Ph.D)
[1]osenisudetu@auchipoly.edu.ng: +234 805 823 1607
[2]adeyeye.sophia@lcu.edu.ng; https://orcid.org/0000-0002-0398-2199: +234 806 112 7708

[1]Department of Office Technology & Management, Auchi Polytechnic, Auchi, Nigeria
[2]Department of Information Management, Lead City University, Ibadan, Nigeria

Abstract

The modern office environment has become increasingly data-driven, creating new ethical, privacy and security challenges. In today's office environment, ethical practices, data privacy and information security are increasingly recognized as critical pillars for organizational effectiveness. This article examined how ethics, data privacy and security function as interdependent pillars in sustaining productivity, compliance and trust in predicting job satisfaction and task completion rate among office workers in Auchi Polytechnic, Auchi. Drawing from both global standards (ISO/IEC 27001:2022, GDPR) and Nigeria's Data Protection Act (NDPA, 2023), the paper integrated theoretical perspectives from Protection Motivation Theory (PMT) and Socio-Technical Systems Theory. Using an empirical review of studies on workplace ethics, data protection and information security, the discussion highlighted how ethical climates influence compliance behaviour, how privacy frameworks guide lawful processing and how everyday security practices safeguard organizational data thus predicting job satisfaction and task completion rate among office workers. A structured questionnaire was administered to 40 respondents across the institution. Data were analyzed using descriptive statistics. Findings suggested that ethical workplace climate, data privacy awareness and robust security practices significantly and positively predict job satisfaction and task completion. The study underscored the need for continuous staff training, organizational compliance with the Nigeria Data Protection Act (NDPA 2023) and integration of ethical and security policies into office management practices.

Keywords: Ethics, Data Privacy, Security, Office Environment

Word Count: 209

Introduction

The 21st century office has evolved into a highly digitalized environment where sensitive information ranging from employee records to financial data flows continuously across systems. The increasing adoption of cloud computing, artificial intelligence and e-learning platforms

intensifies the importance of ethics, data privacy and security (Gürses & Van Hoboken, 2018). In Nigeria, these concerns have gained prominence with the passage of the Nigeria Data Protection Act (2023), which institutionalizes lawful data processing and strengthens the mandate of the Nigeria Data Protection Commission (NDPC).

Ethics is the branch of philosophy that deals with moral principles guiding human behaviour toward what is right or wrong. It influences personal decisions, social norms and legal systems. Ethics is essential in various fields including business, medicine, information management and technology. Ethics evolves with societal changes, but its core purpose remains to guide human actions toward fairness, justice and integrity (Kaptein, 2023). Data ethics on the other hand, refers to the moral principles that guide the collection, use, sharing and storage of data. It is the branch of ethics that evaluates data practices with respect to principles of fairness, accountability and respect for privacy. It encompasses the ethical issues related to data collection, analysis, dissemination and use, ensuring that data-driven activities do not harm individuals or society (Peter, 2024; Moallem, 2022). As digital technologies advance, ethical concerns surrounding data privacy, security and fairness have become more critical. Ensuring data privacy, security and protecting employee information are paramount in today's digital workplace. Best practices for data security include implementing strong access controls, encrypting sensitive information, and regularly updating security protocols.

The modern office environment is increasingly shaped by digital transformation, globalization, and regulatory compliance demands. Ethical practices, data privacy and information security are no longer peripheral issues but fundamental elements that define organizational credibility and effectiveness (Floridi, 2022). In Nigeria, the enactment of the Nigeria Data Protection Act (2023) and the National Data Protection Regulation (NDPR, 2019) has elevated the discourse on privacy and information governance in offices. Ethics, privacy and security are not isolated; together, they form the foundation for accountability, employee trust and compliance in modern offices. Beyond rules and controls, ethical climates (shared perceptions of “how we do things here”) shape whether employees follow security policy or cut corners.

This study seeks to empirically examine the impact of ethics, data privacy awareness and security practices on employees' outcomes such as job satisfaction and task completion rate among office workers in Auchi Polytechnic, Auchi.

Aim and Objectives

The aim of this study is to examine the impact of ethics, data privacy awareness and security practices on employees' job satisfaction and task completion rate among office workers in Auchi Polytechnic, Auchi. Specifically, the study will:

1. Examine how ethical practices influence office productivity and trust (job satisfaction) in Auchi Polytechnic, Auchi.
2. Find out the level of awareness and compliance with data privacy policies among office workers.
3. Ascertain how data security measures affect employees' job satisfaction and task completion.
4. Identify challenges hindering effective integration of ethics, privacy and security.

Research Questions

The following questions are raised to guide the study:

1. How do ethical practices influence office productivity and trust (job satisfaction) in Auchi Polytechnic, Auchi?
2. What is the level of awareness and compliance with data privacy policies among office workers?
3. How do data security measures affect employees' job satisfaction and task completion?
4. What challenges hinder effective integration of ethics, privacy and security?

Conceptual Review

Ethics in the Office Environment

Ethics in the office environment refers to the principles and moral values that guide behaviour, decision-making and interpersonal relationships in professional settings. Ethical workplaces promote trust, collaboration and productivity while fostering a positive organizational culture. Upholding ethical standards is vital for fostering a positive culture in the workplace. Ethics in the

office environment is critical for building a sustainable and trustworthy organization. By promoting integrity, diversity and accountability while addressing ethical challenges, workplaces can create a culture that benefits employees and the organization as a whole. As recent research suggests, ethical practices are not only a moral obligation but also a strategic advantage in today's competitive landscape (Taylor & Bright, 2022).Ethical workplace climate promotes trust, fairness and accountability (Kaptein, 2023). Studies show that ethical leadership fosters employee engagement and reduces misconduct (Treviño, Den Nieuwenboer & Kish-Gephart, 2020).Ethics refers to the moral principles guiding professional behaviour. In office management, ethical practices determine how information is collected, stored and shared (Kaptein, 2023). Ethical climates influence whether staff adhere to information security policies (Yazdanmehr & Wang, 2021). Poor ethical leadership, on the other hand, often correlates with increased data breaches and policy violations.

Data Privacy Awareness

Data privacy refers to the ethical and legal practices of collecting, storing and using data. It involves protecting personal information from misuse and ensuring transparency about how data is processed. Data privacy is the protection of individual's personal information, ensuring that it is handled in a way that respects their rights and maintains their confidentiality. It involves the control individuals have over their data, including how it is collected, used, disclosed and retained (McCarthy & Huang, 2023). Data privacy is significant because it allows individuals to maintain autonomy, trust and control over their personal information. In today's digital landscape, data privacy has become increasingly complex due to the vast array of data collection practices and technologies available. From online shopping to social media interactions, individuals generate an abundance of data that can be used to create detailed profiles and potentially intrude upon their privacy. An example of data privacy is safeguarding employees' social security numbers or customer credit card details. Respecting data privacy builds trust and improves compliance with global regulations. With the growing volume of digital information, data privacy is central to organizational resilience. Privacy concerns influence employees' trust and compliance behaviour (Martin & Murphy, 2017). In Nigeria, NDPR and NDPA (2023) mandate organizations to handle employee and client data responsibly. Data privacy is the right of individuals to control how their personal information is collected and used. Frameworks like the GDPR (2018) and Nigeria's

NDPA (2023) emphasize consent, transparency and accountability. In office environments, privacy is crucial when handling staff bio-data, client information and communication records. Studies show that employee awareness of privacy rights improves compliance and reduces organizational risk (Bélanger & Crossler, 2019).

Security Practices

Data security involves implementing measures to protect information from unauthorized access, alteration or destruction. It focuses on safeguarding data against unauthorized access, breaches or manipulation(s). It involves implementing measures to protect data from threats, such as cyber-attacks, unauthorized disclosures or accidental loss (Shore, 2022). Data security ensures the integrity, availability and confidentiality of data throughout its lifecycle. In an interconnected world, data security is of paramount importance. Breaches and unauthorized access can lead to significant harm, including identity theft, financial fraud, reputational damage and erosion of trust (Taylor & Morgan, 2024). Effective data security measures such as encryption, access controls and regular audits, are crucial to protect sensitive information. Cyber-security practices such as secure passwords, phishing resistance and access control protect organizations from data breaches. Employees' security behaviour significantly impacts organizational vulnerability (Herath & Rao, 2019).Security is the protection of data against unauthorized access, loss or corruption. Standards such as ISO/IEC 27001:2022 provide guidelines for establishing an Information Security Management System (ISMS). In offices, security practices include encryption, access control, password hygiene and phishing awareness. Empirical studies demonstrate that consistent application of security protocols significantly enhances task completion and operational efficiency (Ifinedo, 2021).

Ethics, Data Privacy, Security and Job Outcomes in the Office Environment

In the digital age, protecting data privacy and ensuring robust security are essential in office environments. Organizations handle sensitive information daily, including employee details, client data and proprietary information. Without proper safeguards, breaches can lead to financial loss, reputational damage and legal consequences.

In the workplace, ethics, data privacy and security are interconnected aspects that ensure responsible handling of information, protect stakeholders and maintain a trustworthy professional environment (Sharma & Gupta, 2024). As discussed earlier, ethics in the workplace involves moral principles guiding professional behaviour which ensures fairness, integrity and accountability in all office dealings. Data privacy is the protection of sensitive and personal information from unauthorized access or misuse. Data security on the other hand, involves protecting company and personal data from cyber threats, breaches and unauthorized access. When these three (ethics, data privacy and security) are integrated, organizations can foster a responsible work culture, preventing legal risks and maintaining the trust of employees, clients and stakeholders. Research suggests that ethics, privacy and security policies not only protect organizations but also enhance job satisfaction and task performance (Belanger & Crossler, 2019).

Theoretical Framework

This study is grounded in the Socio-Technical Systems Theory. The Socio-Technical Systems Theory emerged from the Tavistock Institute of Human Relations in the 1950s (Trist & Bamforth, 1951). The theory which was propounded by Emery and Trist in 1960 emphasizes the interdependence between the social system (people, culture, communication, organizational structures) and the technical system (tools, machines, processes, technologies) within an organization. Applied to the modern office, the social subsystem embodies the ethical climate, leadership behaviour and employee values that shape data handling practices, while the technical subsystem encompasses the technological infrastructure, privacy frameworks and security tools that enable safe information processing. The central idea is that effective organizational performance and job satisfaction can only be achieved when both systems are jointly optimized. Simply improving technology without considering human and organizational factors often leads to failure. In information systems, Socio-Technical Systems Theory explains why IT projects succeed or fail based on how well they balance technical efficiency with user needs.

The relevance of the theory to this study is that ethics, data privacy and security operate as interdependent pillars that require joint optimization to sustain productivity, compliance and trust. An ethical climate promotes responsible data behaviour, privacy frameworks ensure lawful and

transparent processing and security practices safeguard organizational data. The synergy of these elements reflects the socio-technical balance essential for a resilient and trustworthy digital workplace.

Empirical Review

Several empirical studies have established the importance of the three pillars:

Ethics and Productivity: A study was carried out by Elegunde et al (2023) on ethical leadership and employees' performance in Lagos State Government offices. The descriptive survey design was used. The population was 381 employees and purposive sampling was used. Data were collected via a structured Likert-scale questionnaire (5-point). Content validity was used and the Cronbach's alpha was used to ascertain the reliability which was 0.875. Result shows that ethical leadership significantly and positively influences employee effectiveness, job satisfaction and productivity. Because employees perceive fairness, respect, etc., they tend to be more productive. Implications: In contexts like modern office environments, leadership that models ethical behaviour can raise productivity, especially when employees see consistent ethical norms and practices. Another study was carried out by Xue et al, 2021 on ethical climates and job satisfaction and performance in the banking sector in Turkey. It also adopted a descriptive survey design with a population of 379 employees. Result shows that ethical climates positively correlate with job satisfaction and lower incidences of information security violations. Also, ethical leadership positively influences benevolent and principled ethical climates. Principled climate has a significant positive effect on job performance.

Implications: It suggests that not all ethical climates or perceptions are equally efficacious for productivity: a principled ethical climate (rules, fairness, principled decision-making) seems more strongly tied to performance.

Privacy Compliance: An empirical study emphasizing information privacy and the consumer was carried out in Norway by Presthus & Sorum (2024) to explore how GDPR has affected consumer knowledge, attitudes and privacy practices over five years. Four online surveys over five years, N = 1,293 (in total). Quantitative statistics and qualitative cluster text mining of responses was adopted. Findings reveal that consumers generally have high knowledge about GDPR and technology (cookies, etc.). Attitudes are positive but skeptical (they like their privacy

rights in theory, but doubt actual enforceability or practicality). Also, practice lags emerged as many users do not take action even though aware. Only a minority actively uses their rights or change behaviour significantly. Equally, another research was carried out by Ologbosere & Ayo-Ogunlusi (2025) on information security awareness and effective use of electronic records systems among administrative staff of private universities in Ibadan. Result revealed that information security awareness (user information compliance and behavioural intentions) is used by the administrative staff of private universities in Ibadan.

Implications: Privacy frameworks (like GDPR) increase awareness and formal rights, but turning that into everyday practices is uneven. So, privacy compliance is necessary but not sufficient for ethical climate/trust. Also, in a study carried out by Bélanger and Crossler (2019) on a review of information privacy research in information systems found that data privacy awareness enhances compliance behaviour, particularly in organizations with strong accountability systems.
Implications: In real offices, privacy compliance can impose costs and friction; but also drives process improvements (better documentation, more rigorous reviews). It shows that privacy frameworks work but need supportive infrastructure and resources.

Security Practices: Ifinedo (2021) carried out an exploratory study on understanding information systems security policy compliance on 116 employees in an organization in Czech using qualitative interviews. Result showed that employee adherence to security protocols predicts higher organizational performance. Also, another research was carried out by Ologbosere & Ayo-Ogunlusi (2025) on information security awareness and effective use of electronic records systems among administrative staff of private universities in Ibadan. Result revealed that the level of information security awareness is moderately high among the private universities in Ibadan.
Implications: Reinforces that employees need to believe in both the threat (severity/vulnerability) and believe they can respond effectively. More recent Nigerian studies (Ayo & Adebiyi, 2024) in their research on cyber-security awareness and compliance among Nigerian office workers confirm that poor cyber hygiene among office staff contributes to security breaches.

Conclusively, ethical leadership improves productivity, job performance and effectiveness. Principled ethical climate is particularly valuable. A strong ethical climate builds trust among

employees, encourages compliance with norms, enhances motivation and leads to better performance. Without ethics, other pillars may be undermined by inconsistent behaviour. General Data Protection Regulation (GDPR) and other regulation raise awareness and rights, but actual practice and usage of rights are mixed. Privacy frameworks contribute to trust (customers, employees) and formal compliance. For productivity and sustainable trust, they must be well implemented (clear, usable, not overly costly) and the ethical climate must support doing what is required and not just ticking boxes. Security Practices like risk awareness, social support and beliefs about threat severity/vulnerability are strong predictors of secure behaviours. Security behaviour is the operationalization of the security pillar: it directly impacts protection of data and reduces risk. For trust/compliance/productivity, secure practices must be supported by ethics (e.g. leadership, organizational values) and well-designed technical/organizational systems.

Methodology

The design used for this research was a descriptive study based on survey research method. Survey research is often used to assess thoughts, opinions and feelings. It consists of predetermined set of questions that is given to a sample which is a representative of the larger population (Agbongiasede, 2018). The descriptive was chosen because of its acknowledged strength in fact finding. The population of the study was 132 (one hundred and thirty-two) office workers of Auchi Polytechnic, Auchi, Edo State, Nigeria. The simple random sampling technique was used to select a sample size of 40 (forty) office workers. This represented approximately 30% of the population studied. The choice of 30% sample size is in line with Westfall (2020) who posited that one strategy in ensuring that a sample is a good representative of the population is by making the sample big enough to optimally reduce error.

The instrument for data collection was the questionnaire titled “Survey of Ethics, Data Privacy Awareness and Security (SEDPAS)” and it was divided into two sections – A and B. Section A sought a background information of the respondents such as Sex, Marital Status and Age; while Section B was made up of 16 items designed to elicit responses on the ethical practice, data privacy awareness and security of data within the office environment. The items in Section B of the instrument were raised on a four-point scale response items as follows:

SA – Strongly agree **A** - Agree **D** - Disagree **SD** – Strongly disagree

Face validity was used for the study. The validity of the instrument was ascertained after the instrument has been subjected to scrutiny by two experts from the Department of Information Management, Lead City University, Ibadan. After they critically examined it checking for appropriateness of the content, they gave their comments as to the validity of the instrument. Based on their suggestions and corrections, final copy of the instrument was drawn. The researchers used test-re-test reliability procedure to determine the reliability of the instrument. Federal Polytechnic, Idah, Kogi State was used to conduct a pre-test. The researchers administered the questionnaire on the office workers of Federal Polytechnic, Idah, Kogi State. After two weeks, the same questionnaire was administered to the same set of people. The results of both tests were compared to determine the reliability of the instrument. The copies of questionnaire were administered by the researchers with the assistance of two research assistants. The research assistants were briefed on the purpose of the research and how to administer the instrument. Copies of the questionnaire were administered to the office workers of the polytechnic and were retrieved same day. The whole exercise was done within two weeks. Percentage and mean method was used to answer the research questions.

Results

This section deals with the results obtained from the analysis of data. 40 questionnaires were issued out to the various respondents in their offices and they were all retrieved representing a 100% retrieval rate.

The following results emerged from the demographic data:

a) Females are more among the population study.
b) There are more married respondents among the population study.
c) The respondents that have worked between the ranges of 11 – 20 years are more among the population study

The following are the results from the responses to the four research questions:

RQ1. **Ethics - Productivity and Trust**

It was found that ethical practices influence office productivity and trust positively as staff are satisfied with their job which modestly associate with task completion. Staff who perceive fairness, consistency and safe reporting report higher satisfaction and fewer workflow frictions.

RQ2. **Privacy Awareness and Compliance level**

It was found that the overall privacy awareness/compliance is moderate (mean 3.43) as only 48% have heard of NDPA 2023 and 30% had training in the last year. Risk behaviours still persist as 22% used personal WhatsApp/email for official data in the last three months.

RQ3. **Security - Job Satisfaction and Task Completion**

It was found that data security measures positively affect employees' job satisfaction and task completion. The result revealed that security practices show meaningful positive links with both task completion (51%) and job satisfaction (41%). Practical habits - MFA, screen lock, phishing reporting - map to smoother workflows and higher confidence.

RQ4.**Challenges (from open-ended coding)**

Results revealed that challenges hindering effective integration of ethics, privacy and security range from limited/irregular training (56%); policy–practice gaps (inconsistent enforcement, 41%); tooling constraints (slow systems, lack of password managers, 34%); shadow channels (WhatsApp/email because "it's faster", 29%); and unclear data retention/DSAR processes (21%).

Discussion of Findings

Findings show that ethical practices significantly influence productivity and trust, aligning with Treviño et al. (2020). However, awareness of privacy laws, particularly the NDPA (2023), was low among respondents, confirming Bélanger and Crossler's (2019) argument that awareness is central to compliance.

Data security was positively associated with job satisfaction, corroborating Ifinedo (2021). Yet, challenges remain: limited training, weak policy enforcement and organizational resistance hinder full integration. This echoes Xue et al., (2021), who stressed employee reluctance as a barrier to security policy compliance.

The findings also support and confirm that ethical climate, data privacy awareness and security practices are vital pillars of the modern office environment. Ethical workplace practices foster

trust, which enhances employee satisfaction. Awareness of privacy rights and obligations under NDPA (2023) improves employees' sense of responsibility, thereby facilitating task completion. Similarly, security practices protect organizational assets and reduce stress, contributing to employee satisfaction.These results align with Kaptein(2023) but extend them into the Nigerian office context, where legal compliance and ethical practices remain evolving.

The empirical evidence suggests that ethics, privacy and security are deeply intertwined. An ethical climate motivates employees to respect data policies, while privacy frameworks provide legal boundaries within which data should be handled. Security mechanisms then operationalized these principles by providing technical safeguards. In the Nigerian context, compliance with the NDPA (2023) is no longer optional; organizations must appoint Data Protection Officers, maintain Records of Processing Activities (RoPA) and conduct Data Protection Impact Assessments (DPIAs). However, compliance will remain superficial if not underpinned by ethical leadership and reinforced by security practices.

Globally, failures in any of the three pillars have led to reputational damage. For instance, unethical data use in Cambridge Analytica's case (Isaak & Hanna, 2018) highlighted how neglect of privacy and security erodes trust. Offices in Nigeria can learn from such cases by embedding ethics, privacy and security into routine workflows.

Findings also confirm that ethics climate, privacy awareness and everyday security practices are each significant predictors of office performance and well-being. Ethical climate reduces violations and boosts job satisfaction; privacy literacy reduces compliance anxiety; secure practices protect workflows. Together, these form a socio-technical foundation for modern office resilience. The three pillars - ethics, privacy, security - each add unique value. An ethical climate reduces policy violations and normalizes "doing security the right way," which lifts job satisfaction. Privacy literacy (aligned to NDPA rights and lawful processing) reduces friction with data subjects and compliance anxiety, nudging both satisfaction and throughput. Secure daily habits (e.g., MFA, least privilege, quick incident reporting) directly protect task flow by preventing disruptive incidents. Together, these pillars form a socio-technical system stronger than any single rule or tool.

Implications

Policy: Nigerian organizations must integrate NDPA compliance with international best practices (e.g., ISO/IEC 27001).

Practice: Managers should foster ethical leadership, build employee capacity in data handling and implement robust ISMS.

Research: Future empirical studies should use longitudinal data to test causal relationships between these pillars and office performance.

Conclusion

Ethics, data privacy and security are indispensable pillars of modern office environments. In Auchi Polytechnic, ethics promotes trust and productivity, but awareness of data privacy laws remains poor. Security measures foster job satisfaction, though challenges of training and enforcement persist. Ethics sets the tone, privacy sets the rules and security executes the routine. Ethics, data privacy and security are interdependent pillars sustaining the modern office environment. Together, they ensure trust, compliance and efficiency. Organizations that institutionalize these pillars will not only achieve regulatory compliance but also enhance employee well-being and productivity. Therefore, ethics, data privacy and security are indispensable for sustaining job satisfaction and improving task completion among office workers.

Recommendations

The study recommended that the management of Auchi Polytechnic, Auchi should:

1. Foster a strong ethical culture through leadership by example so as to enhance high productivity and trust.
2. Institutionalize ethical training and transparent leadership practices as well as provide regular workshops on ethics and data privacy compliance in order to improve the level of awareness and compliance with data privacy policies among office workers.
3. Align policies and strengthen compliance with NDPA (2023) and global best practices as well as invest in advanced security infrastructure and cyber-security awareness programmes.

4. Enforce policies consistently to reduce resistance and ensure integration. Also, management should establish/reinforce regular training programmes and consistent enforcement of policy-practice in order to fill the gap.

References

Agbongiasede, A. E. (2018). Self-employment: An option for professional secretaries in Nigeria. *Journal of Contemporary Business Education Research,* 1(1), 25-30.

Ayo, C. K., & Adebiyi, A. A. (2024). Cyber-security awareness and compliance among Nigerian office workers. *African Journal of Information Systems*, 14(2), 45–60.

Bélanger, F., & Crossler, R. E. (2019). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 43(1), 1–30.

Elegunde, A., Omolara, O. T. & Abimbola, M. (2023). Ethical leadership and employees' performance in Lagos State Government offices. *Journal of Business Economics, Communication and Social Sciences*. 5(3), 177 – 187

European Parliament and Council. (2018). Regulation (EU) 2016/679 (General Data Protection Regulation). *Official Journal of the European Union*, L119, 1–88.

Federal Republic of Nigeria. (2023). *Nigeria Data Protection Act, 2023*. Abuja: Government Printer.

Floridi, L. (2022). The ethics of information. Oxford University Press.

Gürses, S., & Van Hoboken, J. (2018). Privacy after the GDPR. *International Data Privacy Law*, 8(1), 3–12.

Herath, T., & Rao, H. R. (2019). Protection motivation and deterrence: A framework for security policy compliance. *European Journal of Information Systems*, 18(2), 106–125.

Ifinedo, P. (2021). Understanding information systems security policy compliance: An integration of the theory of planned behavior and protection motivation theory. *Computers & Security,* 31(1), 83–95.

International Organization for Standardization. (2022). ISO/IEC 27001:2022 - Information security, cyber-security and privacy protection - Information security management systems - Requirements. Geneva: ISO.

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer,* 51(8), 56–59.

Kaptein, M. (2023). The moral entrepreneur: A new component of ethical leadership. *Journal of Business Ethics*, 156(4), 1135–1150.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), 469–479.

Martin, K., & Murphy, P. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135–155.

McCarthy, T. and Huang, Y. (2023). Data privacy as a trust-building tool. *Journal of Organizational Ethics*, 6 (2), 49 – 63.

Moallem, A. (2022). Privacy vs. monitoring in the digital workplace. *Cyber-psychology Review*, 4 (2), 78 – 91.

National Information Technology Development Agency. (2019). *Nigeria Data Protection Regulation (NDPR)*. Abuja: NITDA.

Ologbosere, O. A. & Ayo-Ogunlusi, V. A. (2025). Information security awareness and effective use of electronic records systems among administrative staff of private universities in Ibadan, Oyo State, Nigeria. *International Journal of Research and Innovation in Social Science (IJRISS)*. 9(14), 1991 – 2000. ISSN No. 2454-6186 / DOI: 10.47772.

Peter, S. (2024). *Encryption technologies for data security*. Data Security Innovations.

Presthus, W. & Sorum, H. (2024). Five years with the GDPR: an empirical study emphasizing information privacy and the consumer. *International Journal of Information Systems and Project Management*. 12(3), 5 - 25

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114.

Sharma, V. and Gupta, A. (2024). Cyber-security strategies for modern enterprises. *Journal of Information Security*, 5 (2), 12 – 25.

Shore, L. M. (2022). Diversity and inclusion in the workplace. *Organizational Psychology Review*, 7 (4), 450 – 460.

Taylor, E. and Bright, P. (2022). The role of ethics training in organizational success. *Journal of Business Ethics*, 4 (1). 322 – 331.

Taylor, E. and Morgan, P. (2024). The impact of cyber-security training on employee behaviour. *Cyber Education Journal*, 4 (1) 256 – 270.

Treviño, L. K., Den Nieuwenboer, N. A., & Kish-Gephart, J. J. (2020). (Un)ethical behavior in organizations. *Annual Review of Psychology*, 65, 635–660.

Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the longwall method of coal-getting. *Human Relations*, 4(1), 3–38.

Westfall, W. J. (2020). *Faculty based practices using blended learning in e-learning and face-to-faceinstruction*.http://www.uwex.edu/disted/conference 24th February, 2020.

Xue, B., Liang, H., & Xie, H. (2021). Ethical leadership and employee compliance with information security policy: *A multilevel model*. *Information & Management*, 58(7), 103119.

Yazdanmehr, A., & Wang, J. (2021). Employees' information security policy compliance: A meta-analytic review. *Information & Management*, 58(6), 103–125.