Teaching Maqasid Al-Shariah Through Case-Based Learning: A Framework for Digital Literacy and Cybersecurity Ethics

Farah Safura Muhammud*

Academy of Contemporary Islamic Studies, Universiti Teknologi MARA (UiTM), Terengganu Branch, Malaysia

***Corresponding Author**

DOI: https://doi.org/10.47772/IJRISS.2026.101000278

Received: 13 October 2026; Accepted: 18 October 2026; Published: 01 November 2026

ABSTRACT

Digital technologies have increased the demand for digital proficiency, critical assessment of online information and responsible financial behaviour. This conceptual paper seeks to explore the possibility of Maqasid al-Shariah to inform the teaching and learning of IMU255 (Property Crimes in Islam). The focus will be on the preservation of intellect (hifz al-'aql) and property (hifz al-mal). The paper organises key digital threats such as misinformation, digital manipulation, harmful online content, phishing, investment scams, romance scams and misuse of personal data through a Maqasid-based lens, based on pedagogical reflection on teaching cyber-related topics. It proposes a case-based approach where students identify the threat, assess its consequences, link it to relevant Maqasid objectives, and justify preventive responses according to Islamic ethical principles and appropriate digital-safety practices. The paper advocates a digital literacy that goes beyond the mere technical awareness to develop students' ability to verify information, recognise manipulation, protect financial and personal data and behave responsibly online. The framework provides a conceptual resource for teaching and learning that integrates Islamic legal ethical reasoning and contemporary cyber threat awareness. Being a conceptual paper, it presents a pedagogical framework and does not provide measured learning outcomes.

Keywords: Maqasid al-Shariah; teaching and learning; case-based learning; online literacy; cyber security ethics.

INTRODUCTION

Digital technologies shape the way people communicate and get information, how people manage money and engage in public life. These developments hold both promise and peril for education. Misinformation, manipulated digital content and harmful online material can influence how people think and make decisions, while phishing, investment scams, romance scams and data theft can compromise financial security. For students of Property Crimes in Islam, these are not just technical problems, but also questions of harm, trust, accountability, honesty and the protection of human welfare.

Maqasid al-Shariah offers an Islamic framework to tackle modern digital challenges in relation to the goals of Islamic law, such as the protection of intellect and property (Auda, 2008; Kamali, 2008). Hifz al-'aql provides a lens through which to understand information integrity, misinformation, digital manipulation and harmful media online. The protection of property is a basis for the analysis of online fraud, phishing, investment scams, romance scams and the protection of digital possessions and personal data. These links provide a significant opportunity to integrate online literacy with Islamic legal and ethical reasoning.

From a teaching-and-learning perspective the challenge is to move students beyond the listing of online dangers to analysing their consequences, identifying the Maqasid objectives at stake and justifying practical and ethical responses. Online literacy here implies verifying information credibility before reposting, identifying manipulative content, safeguarding one's personal and financial information, and understanding the ethical consequences of one's online activities. These are proposed pedagogical applications of the conceptual analysis, not claims of experientially validated learning gains. The critical evaluation of online information is particularly

relevant as research on fake-news identification links source evaluation and evidence-based reasoning to critical thinking (Machete & Turpin, 2020).

This paper investigates how hifz al-'aql and hifz al-mal can serve as a pedagogical lens to contextualise the instruction of digital threats in IMU255; how a case-based learning sequence can link Islamic legal-ethical concepts with online literacy; and what learning activities and assessment criteria may enable students to articulate reasoned, responsible responses to cyber risks.

THEORETICAL FRAMEWORK

Maqasid al-Shariah are the objectives and underlying purposes of Islamic law. It is usually discussed under the preservation of religion, life, intellect, lineage and property. As an analytical lens, Maqasid can help learners to determine whether actions protect human welfare or create preventable harm. A systems-oriented approach encourages thinking about context, relationships and consequences rather than considering a principle as an isolated definition (Auda, 2008).

Hifz al-'aql is the protection and development of the human mind. In the digital realm, it can help guide conversations around online comments, misinformation, fake images and video, and harmful material. The Islamic concept of tabayyun (verification of information before acting on or sharing it) provides a practical bridge to the information literacy. Students can track a claim back to its original source, compare independent sources and differentiate evidence from opinion. Studies on fake news stress the significance of understanding how deceptive information is discovered and disseminated (Machete & Turpin, 2020; Pennycook & Rand, 2021). Therefore, digital-literacy education can make verification strategies explicit instead of assuming that the frequent use of technology automatically leads to critical competence (Audrin & Audrin, 2022).

Hifz al-mal – Protection of property and wealth. Digital banking, e-wallets and e-commerce are convenient but can expose users to phishing, impersonation, investment scams and misuse of personal information. The prior work has also examined cybersecurity through the lens of Maqasid al-Shariah (Osman et al., 2021). The National Institute of Standards and Technology (NIST, 2024) defines cybersecurity as risk management, including identifying risks, protecting systems, detecting incidents, responding and recovering. Students can be taught how to spot warning signs, not to share authentication details and to check platforms themselves.

The paper emphasises hifz al-'aql and hifz al-mal because the course context is about property crimes and digital cases also raise questions about information quality and judgement that can precede harmful action. These two goals offer a targeted teaching pairing: hifz al-'aql underscores the epistemic and cognitive harms, while hifz al-mal underscores the financial assets and property-related harms. They are not meant to be exhaustive of all maqasid objectives.

The mapping is harm-based it's not a fixed one-threat/one-objective classification. For example, a romance scam can be a manipulation of trust and judgement (a concern related to hifz al-'aql) but also a loss of money (hifz al-mal). Students must identify primary and secondary harms, cite evidence from the scenario, and explain why both objectives apply.

Existing scholarship links Maqasid al-Shariah and Islamic ethics to digital competency and digital-ethics education. For example, Ahmad et al. (2025) discuss the principles of Islamic ethics and Maqasid regarding digital competency of adolescents and Mentari et al. (2026) build a conceptual framework for digital-ethics learning from the perspective of Islamic education. The present paper does not, therefore, claim this general relationship to be new. More narrowly, the course-level operationalisation of digital risks into a connected sequence of Maqasid objectives, learning outcomes, classroom tasks, student outputs and assessment criteria.

Research Gaps

The literature found for this paper suggests an increasing interest in Islamic digital ethics, Maqasid-based digital education and ethical digital competency. Ahmad et al. (2025) discussed the principles of Islamic ethics and Maqasid al-Shariah for adolescents' digital competency. Mentari et al. (2026) proposed a learning framework of digital ethics from the perspective of Islamic education. These works make it clear that Islamic values and digital

learning are already being talked about. Therefore, a justifiable research gap has to be tighter than the absence of previous studies.

The gap addressed here is pedagogical: broad discussions of Maqasid and digital ethics need to be actionable in course design through explicit learning stages, observable student outputs and transparent assessment criteria. This focus is in line with reviews that advocate for clearer conceptualisation and intentional development of critical electronic literacy in educational contexts (Audrin & Audrin, 2022; Ilomäki et al., 2023).

This gap statement is provisional, as it is based on a targeted search of relevant literature and not a systematic review. Before submission of the journal, authors should do a documented search of databases such as Scopus, Web of Science and ERIC, define search terms and date limits, and compare the proposed sequence directly with the closest prior frameworks**.**

Novelty And Contribution

What is new in this paper is not the general claim that Maqasid al-Shariah can serve as a guide for digital ethics. Instead, it is a content-faithful pedagogical mapping of the two central objectives, hifz al-‘aql and hifz al-mal, onto the actual digital-risk themes discussed by the students and then suggested case tasks and assessment criteria. In this context, each topic is expressed as a learning opportunity, e.g. verifying a viral claim under hifz al-‘aql, or analysing a phishing message under hifz al-mal. These are suggested instructional uses, not results demonstrated.

The proposed contribution is three-fold. First, it connects two Maqasid objectives to contemporary contexts of information integrity and financial security. Secondly, it identifies classroom activities that make students’ ethical reasoning visible, such as source verification, phishing analysis and scenario-based discussion. Third, it offers assessment dimensions—conceptual accuracy, risk identification, evidence use, ethical justification and communication—that instructors can adapt and test. These contributions make the framework more instruction-oriented than a general digital threats discussion, remaining a proposal that needs empirical validation.

Framework Development and Approach

Thematic Analysis and Design of the Maqasid-Based Framework

A theory informed thematic analysis was used as a conceptual organising procedure to identify recurring themes of digital-risk and link them to the objectives of Maqasid al-Shariah. The analysis was informed by the paper’s emphasis on hifz al‘aql (preservation of intellect) and hifz al-mal (preservation of property). Nor was it an empirical qualitative analysis of interview transcripts, focus group discussions or systematically coded student responses.

The analysis was conducted in four phases. First, the digital-risk topics represented in the course-based material were identified, including misinformation, digital manipulation, excessive technology use, phishing, investment scams, romance scams and misuse of personal data. Second, we examined each topic for its potential harm, who it might harm and how it might harm them. Third, the topics were classified as hifz al-‘aql, hifz al-mal or both, in accordance with the type of possible harm. Fourth, each thematic category was translated into a proposed learning outcome, classroom activity, expected student output and assessment criteria.

Two general themes for analysis were identified. The first, information integrity and judgement, includes misinformation, digital manipulation and potentially harmful patterns of technology use. It is mainly concerned with hifz al‘aql since these risks may hinder the capacity to assess information, make judgement and take responsible decisions. The second is financial security and protection of digital information and includes phishing, investment scams, romance scams, and misuse of personal data. It is primarily associated with hifz al-mal as these risks may put property and financial assets at the risk of loss. The themes are not mutually exclusive, but analytically related. For example, an investment scam may use false information or emotional manipulation, but it also poses a risk to your financial assets.

The pedagogical mapping in Table 2 was guided by the emerging thematic structure. The themes are a conceptual

synthesis of course-related topics and selected literature. They should not be taken as empirically generated themes based on student interviews, nor as evidence of the prevalence of digital threats. The framework is thus proposed for classroom use and further research is needed through documented teaching implementation and appropriate evaluation.

Table 1. Conceptual thematic structure linking digital risks and Maqasid objectives

Overarching theme	Included subthemes	Primary Maqasid focus
Information integrity and judgement	Misinformation; digital manipulation; excessive technology use	Hifz al-'aql
Financial security and protection of digital information	Phishing; investment scams; romance scams; misuse of personal data	Hifz al-mal
Overlapping harms (cross-cutting analytical principle)	Manipulation or misinformation contributing to financial loss; scams involving emotional pressure and transfer of assets	Hifz al-'aql and hifz al-mal, where justified by case evidence

This paper adopts a conceptual and pedagogical approach based on reflection in the teaching of IMU255 (Property Crimes in Islam) and a focused literature review on Maqasid al-Shariah, online literacy, misinformation, cybersecurity and case-based learning. The framework was developed in four analytic steps. First, we extracted digital-risk themes from the material considered in the course-based conceptual analysis that were relevant to the course context. Second, harms and affected parties in each theme were identified. Third, each theme was mapped to hifz al'aql, hifz al-mal, or both based on the nature of the harm, not the technology. Fourth, the mapping was translated into a learning outcome, classroom activity, and observable student output and assessment criteria. This is an open process of conceptual development, not an empirical intervention nor a validated instructional model.

Changed the first topic map to a pedagogical alignment matrix. Activities included chances for students to produce observable evidence of intended learning, such as a source-check log for information verification or an annotated phishing message for threat recognition. The matrix aligns intended outcomes, learning activities and assessment criteria, in line with constructive alignment (Biggs & Tang, 2011): It's still a reasoned design proposal, and one that should be piloted before claims of effectiveness are made.

Students will be able to: (1) explain the relevance of hifz al'aql and hifz al-mal to digital risks; (2) identify the harm, the party affected and the evidence in a digital case; (3) distinguish risks to information integrity and judgement from risks to property and personal data while recognising overlapping harms; (4) apply tabayyun, amanah, honesty and prevention of harm to a case; and (5) justify a safe, proportionate response using credible sources.

Conceptual Mapping of Digital Literacy to Maqasid-Based Teaching

Table 2. Mapping digital risks to Maqasid objectives, learning outcomes, activities and assessment

Digital-risk category	Maqasid objective(s)	Intended learning outcome	Classroom activity	Expected student output	Assessment criterion
Misinformation / viral claim	Hifz al-'aql; hifz al-mal if it influences a financial decision	Verify a claim and explain how weak evidence can distort judgement or decisions.	Trace the claim to its original source and compare independent sources.	Source-check log with a justified conclusion.	Source credibility, evidence quality and reasoning.
Digital manipulation / harmful content	Primarily hifz al'aql; may overlap depending on harm	Identify manipulation cues and distinguish	Compare a post with its original context and trusted reporting.	Annotated case analysis identifying evidence gaps.	Accurate risk identification; distinguish fact from assumption.

		verified facts from inference.			
Digital addiction / uncontrolled use	Hifz al-'aql and well-being; not a clinical diagnosis	Identify possible effects on judgement, attention or daily responsibilities and propose realistic boundaries.	Discuss a fictional scenario about excessive use and its consequences.	Short reflection and practical boundary-setting plan.	Relevance, practicality and ethical reasoning.
Phishing / impersonation	Hifz al-mal; personal data may expose assets to further harm	Recognise warning signs and select a safe response.	Annotate a fictional suspicious message and identify red flags.	Threat checklist and protective-response steps.	Warning-sign identification and feasibility of response.
Investment scam	Hifz al-mal; hifz al-'aql where misinformation or pressure shapes judgement	Evaluate financial claims and explain risks of acting without verification.	Review a fictional investment pitch and check claims independently.	Risk memo identifying claims, evidence and recommended action.	Evidence quality, recognition of financial harm and justification.
Romance scam	Both hifz al-'aql and hifz al-mal may apply	Explain how emotional manipulation can precede financial exploitation.	Map a fictional conversation to manipulation cues, requests for money and safe next steps.	Case map identifying primary and secondary harms.	Recognition of overlapping harms and reasoned response.
Misuse of personal data	Hifz al-mal where data enable theft; other objectives may also apply	Explain downstream risks of data disclosure and identify protective steps.	Examine a fictional data-sharing scenario and identify minimum necessary disclosure.	Data-protection action plan with justification.	Risk analysis, practical safeguards and ethical reasoning.

Proposed Case-Based Learning Sequence

The proposed case-based learning sequence converts the thematic analysis into a concrete teaching design. It can be taught in one long class or over several sessions, depending on the students' prior knowledge and the scheduling of the course. Each stage has a learning purpose that is intended, and a visible output that can be used to inform formative feedback.

Stage 1: Build a plausible case. Add to that a situation like a strange link claiming government assistance, an investment opportunity promising unrealistic returns, or a viral claim with no verifiable source. Students write down what they know, what they don't know, and what evidence they need. Output: a preliminary checklist of claims and evidence.

Stage 2: Analyse the risk and affected parties. Students break into small groups to discuss who might be harmed, what information or assets are at risk, how the message attempts to influence the recipient and what might happen if it is believed or shared. Students analyse the impact on individuals, families, communities and institutions.

Stage 3: Match the case to Maqasid principles The students determine whether hifz al-'aql, hifz al-mal, or both are involved, and justify their reasoning. An unverified viral claim may raise concerns regarding intelligence and safe sharing. Phishing may directly threaten ownership and private information, manipulating judgement.

Step 4: Evaluate the answers. Groups propose an ethical and practical response, using concepts such as tabayyun, amanah, honesty, justice and prevention of harm. Actions include checking an official source through a separate

channel, refusing to provide one-time passwords, contacting a bank using verified details or reporting suspicious content. NIST's (2024) risk-management approach can distinguish between prevention, detection, response and recovery.

Stage 5. Reflect and transfer. Each student writes a short reflection on what digital action they would do differently and why. The instructor can then present a new scenario to test students' ability to transfer their reasoning to a different context.

The sequence is intended to promote active engagement and a structured way of thinking, and to make the link between Islamic concepts and everyday digital practice explicit. Case-based learning is widely used to place concepts into realistic problems, although its value is related to the design of cases, facilitation and alignment with intended outcomes (Thistlethwaite et al., 2012).

Learning Activities And Assessment

In a source-verification exercise, students follow a claim back to its original source, assess independent sources, and record corroborating or contradictory evidence. Students are asked to identify red flags in a hypothetical phishing message, including suspicious links, requests for authentication codes, urgency and mismatched sender details. A Maqasid mapping task asks groups to match each risk to hifz al-'aql, hifz al-mal or both, and to defend their interpretation. Role play can give students the perspective of a user, a family member, a financial institution, and a community educator.

The aim of assessment is to reward reasoning and evidence, not just memory. A rubric might be used to assess five dimensions: accuracy in explaining Maqasid concepts; quality of identification of risk; use of credible evidence; practicality and ethical justification of the response; and clarity of communication and reflection . Instructors may use written case analysis, group presentation, individual reflection or scenario-based quiz. A single element can disentangle a student's grasp from the group's performance. This alignment of desired outcomes, learning activities and assessment is consistent with constructive alignment (Biggs & Tang, 2011). Case-based and active learning approaches also emphasise the application of concepts to meaningful problems (Prince, 2004; Thistlethwaite et al., 2012).

Assessment criterion	What is assessed	Weight
Maqasid understanding	Accurately explains hifz al-'aql and/or hifz al-mal and their relevance to the case.	20%
Threat and evidence analysis	Identifies the risk, affected parties, warning signs and evidence gaps.	25%
Use of credible sources	Checks claims against reliable sources and distinguishes fact from assumption.	20%
Islamic ethical reasoning	Applies principles such as tabayyun, amanah, honesty and prevention of harm with a reasoned explanation.	25%
Communication and reflection	Presents a clear, practical response and reflects on responsible digital behaviour.	10%

The point of the assessment should be how well students can reason, not how well they can parrot definitions. A formative task might be to ask each group to analyse a fictional viral claim or suspicious financial message, identify the evidence, affected parties, link the case to hifz al-'aql and/or hifz al-mal and justify a safe response. This approach is consistent with constructive alignment, where intended learning outcomes, learning activities and assessment should reinforce each other (Biggs & Tang, 2011). Case-based discussion may also help to apply concepts to realistic scenarios, if the cases and criteria are transparent (Prince, 2004).

Future assessment could consist of comparing student responses to similar scenarios before and after the activity, analysing justifications with a transparent rubric, and obtaining feedback regarding relevance and clarity. Any study must describe its sample, procedure, instruments and analysis, obtain institutional approval if need and not infer behavior change solely from satisfaction. These are suggestions for further research. The source assignment reports did not do any such evaluation.

Table 3. Alignment of intended learning outcomes, student evidence and assessment criteria

Intended learning outcome	Student evidence	Assessment criterion	Suggested weight
Explain hifz al-'aql and hifz al-mal in relation to digital risks	Brief concept explanation and case classification	Conceptual accuracy and relevance	20%
Identify harm, affected parties and evidence	Harm map separating facts from assumptions	Accuracy of risk identification and evidence use	25%
Apply Maqasid and recognise overlapping harms	Written Maqasid-based justification	Reasoned application and handling of overlap	25%
Recommend a safe, proportionate response	Prevention and response plan	Practicality, ethical justification and safety	20%
Communicate the analysis clearly	Oral briefing or case memo	Clarity, structure and appropriate source use	10%

DISCUSSION

The heart of the pedagogical value of this approach is the combination of Islamic legal-ethical reasoning and recognisable digital situations. Teaching should be visible to the original subject matter: fake news and digital manipulation are not the same as scams and hifz al-'aql and hifz al-mal should be explained distinctly even if some cases involve both. For example, a misleading investment message can manipulate judgement, and also threaten money. A phishing message may exploit trust and lead to loss of financial assets or personal information. The educational task is to help learners to examine claims and evidence systematically, rather than relying on intuition or familiarity with digital platforms (Machete & Turpin, 2020; Audrin & Audrin, 2022).The proposed sequence can be seen as a useful route for discussion in the classroom and for formative assessment (Figure 1).

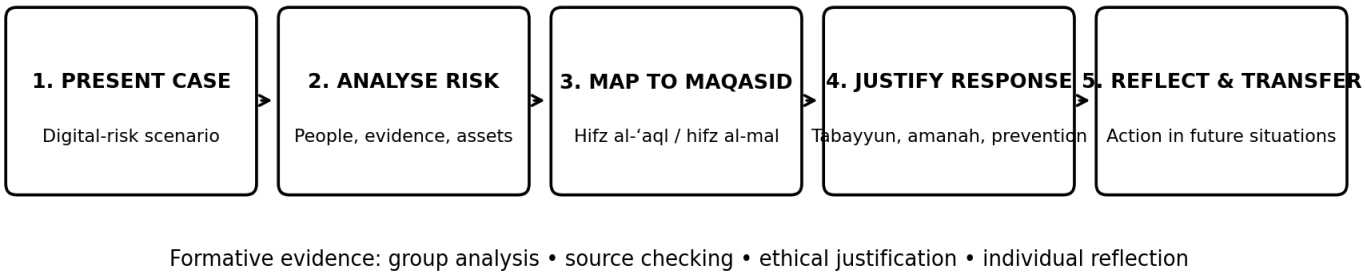

Figure 1. Five-stage case-based learning sequence linking digital-risk analysis with Maqasid-based reasoning (author's conceptual framework).

First, hifz al-'aql is not only about avoiding harmful content. This includes verification of information, resistance to manipulation and rational judgements. Observable learning behaviours translate into tabayyun: tracking down sources, comparing evidence, and suspending judgement when evidence is insufficient. These behaviours are more specific than a blanket instruction to be careful online and so are better teaching targets. They are also related to critical online literacy approaches that emphasise evaluation, reflection, and responsible participation (Ilomäki et al., 2023). Students should describe overlapping cases as having primary and secondary harms and justify the application of both objectives with scenario evidence, rather than forcing each case into an exclusive category.

Second, hifz al-mal is not only about financial assets, but also about information that may lead to their misuse. Students can learn the consequences of clicking on a suspicious link or revealing an authentication code that can result in financial loss. Individual users should not have sole responsibility: institutions need secure systems, clear reporting channels and timely responses.

Third, the approach may help instructors relate Islamic legal-ethical concepts to contemporary contexts. Its value will be dependent on case quality, facilitation, students' prior digital proficiency and the alignment between

learning outcomes and assessment. Scenarios should be culturally appropriate and legal claims verified with authoritative and current sources before being used in the classroom.

The framework is not without its limitations. This is a conceptual proposal based on selected literature and is not a systematic review or classroom study. No student data were collected for the purposes of this article, and the paper does not claim that the proposed activities have improved online literacy, cybersecurity awareness or ethical reasoning. The activities should, next, be piloted, implementation documented and student work assessed with a transparent rubric before the evaluation of learning outcomes. All sources and any use of course related material should be checked against original records and institutional publication requirements as applicable.

CONCLUSION

This paper presents a conceptual teaching-and-learning framework for integrating digital literacy with Maqasid al-Shariah in IMU255 (Property Crimes in Islam). By connecting hifz al-'aql with information integrity and hifz al-mal with financial and personal-data security, the framework encourages students to analyse cyber risks through Islamic legal-ethical reasoning and practical digital-safety habits. Its five-stage case-based sequence and proposed assessment rubric offer a structure for classroom use. Future implementation should be documented and evaluated before claims about effectiveness are made.

Future work should pilot the proposed cases in IMU255, document implementation, assess student explanations using the proposed rubric and obtain any institutional approvals required for research involving students. A subsequent study could compare student reasoning before and after instruction or analyse work samples against predefined criteria, while reporting its design and limitations transparently.

ACKNOWLEDGEMENTS

The author acknowledges the teaching context of IMU255 (Property Crimes in Islam), which prompted reflection on how Maqasid al-Shariah can inform students' analysis of contemporary cyber threats.

REFERENCES

1. Ahmad, N., Ma, M. K., Abd. Rahman, S. F., Syed Mahmood, S. R., Muhamad@ Razak, N. A., & Mohamad, S. N. A. (2025). The Islamic ethical principles and Maqasid al-Shariah to enhance digital competency among adolescents. UMRAN—International Journal of Islamic and Civilizational Studies, 12(3), 101–117. https://doi.org/10.11113/umran2025.12n3.833
2. Auda, J. (2008). Maqasid al-Shariah as philosophy of Islamic law: A systems approach. International Institute of Islamic Thought.
3. Audrin, C., & Audrin, B. (2022). Key factors in digital literacy in learning and education: A systematic literature review using text mining. Education and Information Technologies, 27, 7395–7419. https://doi.org/10.1007/s10639-021-10832-5
4. Biggs, J., & Tang, C. (2011). Teaching for quality learning at university (4th ed.). Open University Press.
5. Ilomäki, L., Lakkala, M., Kallunki, V., Mundy, D., Romero, M., Romeu, T., & Gouseti, A. (2023). Critical digital literacies at school level: A systematic review. Review of Education, 11, e3425. https://doi.org/10.1002/rev3.3425
6. Kamali, M. H. (2008). Maqasid al-Shariah made simple. International Institute of Islamic Thought.
7. Machete, P., & Turpin, M. (2020). The use of critical thinking to identify fake news: A systematic literature review. In Responsible design, implementation and use of information and communication technology (pp. 235–246). Springer. https://doi.org/10.1007/978-3-030-45002-1_20
8. Mentari, I. E. R., Sari, S. F., Nova, M. A. D., Rozy, F., Lubis, A. S., & Dina, S. (2026). Digital ethics-based learning strategies from an Islamic education perspective. Al-Mudarris: Jurnal Ilmiah Pendidikan Islam, 9(2), 325–342. https://doi.org/10.23971/mdr.v9i2.11442
9. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

10. Osman, R. A. H., Zakariyah, L., Zakariyah, H., & Dahlan, A. R. A. (2021). Cyber security and Maqasid al-Shariah: A case of Facebook application. International Research Journal of Shariah, Muamalat and Islam, 3(6), 12–25. https://doi.org/10.35631/IRJSMI.36002
11. Pennycook, G., & Rand, D. G. (2021). The psychology of fake news. Trends in Cognitive Sciences, 25(5), 388–402. https://doi.org/10.1016/j.tics.2021.02.007
12. Prince, M. (2004). Does active learning work? A review of the research. Journal of Engineering Education, 93(3), 223–231. https://doi.org/10.1002/j.2168-9830.2004.tb00809.x
13. Thistlethwaite, J. E., Davies, D., Ekeocha, S., Kidd, J. M., MacDougall, C., Matthews, P., Purkis, J., & Clay, D. (2012). The effectiveness of case-based learning in health professional education: A BEME systematic review. Medical Teacher, 34(6), e421–e444. https://doi.org/10.3109/0142159X.2012.680939