Report and Recommendations
'Alice'
Ethical Considerations for AI in Education

Enzo Joly, 22055453

Module Title: UFCFB5-15-3 | Ethical and Professional Issues in Computing and Digital Media
Word Count: 2,056

Contents

1 Introduction

This report comprises ethical considerations and analysis concerning technology, data privacy, disinformation, and accessibility.

The resulting recommendations for deployment aim to inform, such that TechSoft be fully cognisant of challenges faced by an AI chatbot in education. South Star Academy's proposed student support services chatbot 'Alice' will require thoughtful diligence before it can be deemed production-ready.

2 Relevant Codes of Practice

Professional codes of conduct provide software engineers with an ethical starting point for a deployment of this nature. Given the bandwidth of this topic, and the scope of this report, exhaustive coverage of the full documentation is impossible, so key characteristics of differing guidelines will be the primary focal point. The BCS focusses on professionals; the IEEE standardises the technological aspects; the ACM is more concerned with societal impact.

2.1 BCS Code of Conduct

BCS members must demonstrate "due regard for public health, privacy, security and wellbeing of others and the environment" *(BCS 2024, p. 2)*, particularly salient considering Alice will be handling sensitive student data and potentially influencing student wellbeing.

The BCS also mandates professionals to only provide service "within [their] professional competence" *(BCS 2024, p. 2)*, which begs the question: where exists the limit of Alice's 'competence' in the context of student support? Is a system's competency assumed to be an extension of the professionals who calibrated it?

Members are additionally required to "uphold the reputation of the profession" *(BCS 2024, p. 3)*. This translates to full transparency regarding Alice's management and capabilities. Safeguards must also be in place to prevent misuse in order to preserve public trust of AI systems in education, let alone the trust of students.

2.2 IEEE Code of Ethics

Data retention and deletion policies must be established and clear, ensuring a commitment to "protection of... personal information and data" *(IEEE 2024, p. 1)*, and a commitment to student privacy. Engineers must identify and eliminate potential bias from the model and algorithms in use, such that Alice "not discriminate against any person because of characteristics protected by law" *(IEEE 2024, p. 1)*. This should be verified and assured with rigorous testing and regular audits, ensuring commitment to "honest and realistic... claims or estimates based on available data" *(IEEE 2024, p. 2)*, coupled with an established mechanism for human oversight and intervention when Alice's confidence in a response is low.

2.3 ACM Code of Ethics

The ACM Code proposes that "all people are stakeholders in computing" *(ACM 2024a, p. 1)*, alluding that the enhancement of student wellbeing and academic success is not merely a nice gesture, but necessary for the betterment of society, assuming compliant (and considerate) execution.

Alice should be constructed with accessibility in mind, "[fostering] fair participation of all people, including those of underrepresented groups" *(ACM 2024a, p. 2)*.

Caveats to Information Processing

Blundell argues that "such codes are seldom consulted and often incorporate bland (and sometimes contradictory) statements intended to satisfy a broad range of stakeholders" *(Blundell 2020, p. 40)* and professionals must practise discernment and maintain awareness for the consequences of poor decision-making, both quantitatively and in qualitative aspects. Underpinning deontological ethics is the notion that the professional is duty-bound to rely on their better judgement where universally established rules fail. Duty to reason is one of the core beliefs that make up Kant's philosophical tenet, "respect the reason in you."

The BCS specifies duty to "due... diligence in accordance with the Relevant Authority's requirements whilst exercising... professional judgement at all times" *(BCS 2024, p. 2)*. In context: information relating to the endangerment of any student(s) takes precedent over privacy, as is established protocol *in loco parentis*, at the discretion of human moderators. Sophisticated content-flagging and de-identification secured by multiple key-holders will ensure awareness and consensus for de-anonymisation. Students may be more comfortable anonymously, so this process of de-anonymising must be abuse-proof to ensure trust remains strong.

All decision-making processes must prioritise students foremost, with the necessary privacy precautions in place to protect student data alongside regular monitoring of the chatbot's holistic impact on the educational environment.

3 Further Considerations

A Note on Regulatory Standards

In-depth representation for truly ethical and compliant practice are appended in Appendix B (relevant definitions with respect to implications for Alice), and not the main body of this report, for brevity's sake.

3.1 Ethical Data Governance

Any implementation of Alice would raise significant privacy concerns regarding the collection, storage, and use of student data *(Annus 2024, pp. 366-370)*. In the best interest of both students and the law, all-encompassing singular actions, policies, and processes have the potential to satisfy the needs of all stakeholders simultaneously. Proper management of data involves:

3.1.1 GDPR/Regulatory Compliance

From design through to deployment continuously for any collection of data, as well as full transparency in its use of data, and clarity regarding what it is collecting data to be used for, TechSoft must define the nature of its policies, processes, and practice. It is also imperative that TechSoft safeguard against any third-parties from gaining access to data with security best practices. Schools are in position to safeguard student data, appreciating this perspective is essential for TechSoft engineers. For more information, see Appendix B. Additionally, record a Data Protection Impact Assessment (DPIA) and keep it up to date (template provided in Appendix A).

3.1.2 Data Security

Privacy by design as an ethos enabling strong governance and security measures; OAuth 2.0 and OpenID Connect for Single Sign-On (SSO) and Role-Based Access Control (RBAC) for fine-tuning permissions *(Josuttis 2024, pp. 80-120)*. Data encryption *(Stallings 2024, pp. 100-150)*, AES-256 for data at rest and TLS 1.3 for data in transit.

3.1.3 Data Anonymisation

K-anonymity employed for protecting student identities *(Emam 2024, pp. 75-100)*, and the implementation of differential privacy for aggregate data analysis, anonymising students entirely into statistics beneficial for upgrading and improving the chatbot, and alleviating the burden of at-risk data unnecessary for development purposes.

3.1.4 Data Minimisation

Information about data usage must be clear, with opt-in mechanisms for non-essential features and informed consent for all users/guardians concerned. In the context of students, it is vital to ensure that data is only collected when necessary, and that it is stored securely and "audited regularly to ensure all stored information is still relevant" *(A29WP 2018)*, implementing "privacy-preserving UX patterns" *(Hartzog 2024, pp. 50-100)*, making privacy settings easily accessible and understandable.

3.2 AI Ethics Principles

Principled practice is a must, adhering to established AI ethics principles *(EC 2024)*:

3.2.1 Ethical Algorithm Design

Explicit labelling of Alice as an AI system *(IEEE 2024)*, prioritising the elucidation of users. Understanding algorithmic configuration choices and their consequences can benefit not only developers, but users, and by extension society en masse.

3.2.2 Human Agency and Oversight

Setting "clear boundaries between AI support and human intervention" *(APA 2024)* by defining thresholds for transitioning between human support and AI. Contextual enquiry of staff to better map support scenarios by conducting user research *(Goodman 2024, pp. 50-100)*, alongside human-in-the-loop dialogue optimisation *(Vaughan 2024, pp. 30-60)*. Evaluations can be crowdsourced for diverse perspectives.

3.2.3 Iterative Design Process

An iterative strategy *(Holtzblatt 2024, pp. 30-60)* will aid in the formation of an adaptable system for frequent ethical review *(Floridi 2024)*. Periodic assessment of chatbot bias, plus alignment against ethical benchmarks. Usability testing with representative student groups ensures these needs are measured and met on a regular basis.

3.2.4 Disinformation and Technical Safety

Content-filtering in effect, with established escalation protocols for disinformation or harmful content. Natural and effective chatbot interactions, establishing tone and personality *(Bradbury 2024, pp. 20-50)*, maintaining a consistent voice aligned with an educational context, ensuring age-appropriate content. Harmful or inappropriate chatbot responses *(Bickmore 2021, p. e11510)* accounted for.

3.2.5 Transparency

"Explainable AI techniques to interpret chatbot decisions" *(Arrieta 2022, pp. 82-115)* thanks to interpretable machine learning models and provision of rationale, with respect to design recommendations in the software lifecycle.

3.2.6 Fairness-Aware Machine Learning

"Fairness-aware machine learning" technology *(Barocas 2021)*, tracking algorithm parity fairness metrics. TechSoft must subsume a mindset for mitigation: frequent bias testing, essential for equitable support. Regular bias testing *(ACM 2024b)* including the employment of automated bias-detection tools, in tandem with supervised evaluation.

Diverse training data, to prevent demographic biases *(Mehrabi 2024, pp. 1-35)* is important. Diverse student profiles in training data ensure an inclusive model representative of the entire student demographic.

3.3 Ethical UX Design Patterns

TechSoft must commit to a design process focussed on student needs:

3.3.1 Accessibility Standards

Adhering to WCAG 2.2 *(W3C 2024)*, content can be perceivable, operable, understandable, and considerate of an array of user interaction.

Cognitive accessibility *(Yesilada 2024, pp. 1-10)* with clear and simple language, alongside multilingual options *(Anastasiou 2024, pp. 50-100)* provides consistent layout and interaction patterns.

3.3.2 User-Centred Design

An adaptable user interface *(Harper 2024, pp. 20-50)*, offering customisable font sizes and colour contrasts supporting a range of input (text, voice, video, gestures), and optionally reducing visual clutter to address neurodiversity *(Armstrong 2024, pp. 30-60)* will accommodate special needs.

3.3.3 Dark Pattern Avoidance

Dark patterns *(Brignull 2024)* must be avoided. Operational transparency including information about Alice and data usage, with clear opt-out options for data collection are of utmost importance. Information pertinent to students and their rights must be made crystal clear.

3.3.4 Attention Economy Awareness

This includes also addressing attention economy concerns *(Williams 2024, pp. 10-30)*, designing for focussed, purposeful interactions and avoiding addictive design patterns. This is vital in the context of impressionable and susceptible youth and vulnerable persons.

3.3.5 Psychological Impact

AI Support is liable to psychological impacts as well and these must be considered too. TechSoft must mitigate the risk of over-reliance on AI for emotional support *(Miner 2022, p. 746)*, clearly communicating AI's role as a supplement to (not replacement for) human support. Pre-existing human counselling services can be integrated facilitating non-AI support roles.

3.4 Monitoring, Evaluation, and Continuous Improvement

"Human-centric AI" should be a key principle. TechSoft should co-opt a model of supervised learning for classification tasks (e.g., identifying at-risk students) with the following tools:

3.4.1 Natural Language Processing (NLP) Frameworks

A state-of-the-art chatbot implementation may employ a GPT/Transformer-based, or even BERT model, implementing NLP frameworks *(Jurafsky 2024, pp. 1-15)* simulating an understanding of context and intent in a bespoke service.

3.4.2 Conversational Metrics

Setting up telemetry *(Vadapalli 2024, pp. 30-60)* includes real-time data collection on user interactions, ensuring privacy-preserving logging mechanisms. Once established, however, is an incredibly utile toolchain for measuring conversational metrics *(Quarteroni 2024, pp. 1-32)*. Enabling response accuracy and relevance, and task completion rates, to be tracked in real-time.

3.4.3 Usage Analytics

Common queries and pain points can be identified with usage analytics *(Beasley 2024, pp. 50-100)*, analysing conversation flows and quality. Sentiment analysis *(Liu 2024, pp. 50-100)* can be performed, analysing emotional tone of student interactions.

3.4.4 Research Collaboration

It would be beneficial to foster the academic community, establishing partnerships with universities *(Dillenbourg 2024, pp. 50-100)* for contribution to research, and ensuring the quality of the service. Findings can also be published to contribute to the broader field.

4 Reflection and Recommendations

Throughout the software development lifecycle, encapsulated here: "privacy by design" from the foundation, with "human-centric AI" as a guiding principle to instill responsibility and a "mindset for mitigation." This means optimising for ethical best practice from the foundation up: informed consent built-in, training for all staff, and ultimately assisting the existing school culture to care for students and venerating this ethos above all else. With ethos-driven targets permeating every aspect of its implementation, Alice must also exemplify educational empowerment for cognitive stewardship, empowering students, educators, and support workers alike.

This can only be achieved through strict data handling, management, audit procedures etc. TechSoft must devise training such that it enables staff to work effectively alongside AI systems, as opposed to in lieu, or in spite, of them, all the while upholding accountability as protocol. Transparency can ensure TechSoft a model for "responsible innovation" in educational AI and amongst a sensitive and valued ecology of academia. Compliance, accessibility, and effectiveness will converge naturally through thoughtful design choices to establish a sensible and proactive ethical framework and governance structure.

In combination with adaptive and continuous evaluation, TechSoft can assure a system that truly serves its mission while protecting student interests. Prioritise students. Cater to diverse student needs. Ensure continued compliance with legislature. Complete and maintain an updated Data Protection Impact Assessment, filing and refactoring it according to a robust change policy.

A Appendix A: Data Protection Impact Assessment Template

1. Project Overview

- **Project Name:** AI Chatbot in Education
- **Data Controller:** South Star Academy
- **System Owner:** TechSoft
- **Date of Latest Revision:**

2. Data Processing Activities

1. **Nature of Processing**
   - Collection methods
   - Data flows
   - Retention period and procedure
2. **Scope of Processing**
   - Types of personal data processed
   - Volume, aims and scope
   - Context of processing

3. Necessity and Proportionality

1. **Lawful Basis for Processing**
   - Identify relevant Article 6 GDPR condition
   - Identify Article 9 condition
   - Justification for chosen basis
2. **Data Minimisation**
   - Justification for each data element
   - Retention periods and rationale
   - Privacy-preserving measures
3. **Accuracy Measures**
   - Data quality procedures
   - Update mechanisms
   - Verification processes

4. Risk Assessment

Risk	**Potential Impact**	**Likelihood (H/M/L)**	**Mitigation Measures**
Data Breach	Unauthorised access to student data	H	
Algorithm Bias	Unfair treatment of certain student groups	M	
Mental Health Impact	Negative psychological effects from AI interactions	M	
Data Accuracy	Incorrect support guidance	M	
System Misuse	Exploitation of AI system	M	

5. Data Subject Rights

1. **Information Provision**
   - Privacy notice content
   - Rectification and erasure mechanisms

6. Organisational Measures

1. **Security Standards**
   - Network security
   - Physical security
   - Staff training
2. **Data Protection Measures**
   - Data minimisation controls
   - Purpose limitation safeguards

7. Consultation

1. **Internal Stakeholders**
   - IT Security Team feedback
   - Legal Team review
   - Student Support Services input
   - Senior Management approval
2. **External Stakeholders**
   - Student representative feedback
   - Parent consultation
   - Educational authority guidance
   - DPO recommendations

8. Risk Treatment

Identified Risk	Treatment Measure	Residual Risk Level

1. **Outcome Decision**
    - Proceed with processing: (Y) / (N)
    - Conditions applied:

9. Ongoing Monitoring Plan

1. **Review Schedule**
    - Regular review dates
    - Trigger events for review
    - Responsibility assignments
2. **Monitoring Measures**
    - Performance metrics
    - Incident reporting
    - Audit procedures

10. Sign-off

Information Security Manager:

_____

Signature:

B Appendix B: Regulatory Standards

DATA PROTECTION LEGISLATION

General Data Protection Regulation (GDPR)

"

- Establishing a lawful basis for processing: Consent or legitimate interests
- Implementing data subject rights: Access, rectification, erasure, portability
- Appointing a Data Protection Officer (DPO)

"

(EU 2016)

UK Data Protection Act 2018

"

- Adhering to specific provisions for processing personal data in educational contexts
- Implementing safeguards for processing special category data (e.g., health information)

"

(UKGov 2018):

Children's Online Privacy Protection Act (COPPA)

"

- Obtaining parental consent for students under 13
- Implementing limited data collection and retention policies

"

(FTC 2024)

EDUCATION SECTOR REGULATIONS

Education and Skills Act 2008

"

- Fulfilling the duty to promote the well-being of students
- Implementing safeguarding responsibilities in digital environments

"

(UKGov 2008)

Keeping Children Safe in Education

"

- Implementing online safety measures for educational technology
- Providing staff training on digital safeguarding

"

(DfE 2024a)

Special Educational Needs and Disability (SEND) Code of Practice

"

- Ensuring accessibility requirements for digital learning tools are met
- Considering personalised support for students with SEND

"

(DfE 2024b)

PROFESSIONAL STANDARDS AND GUIDELINES

BCS Code of Conduct

"

- Considering public interest in development decisions
- Maintaining professional competence and integrity
- Fulfilling duty to relevant authorities

"

(BCS 2024, pp. 1-5)

ACM Code of Ethics and Professional Conduct

"

- Contributing to society and human well-being
- Avoiding harm in system design and implementation
- Maintaining honesty and trustworthiness

"

(ACM 2024a, pp. 1-4)

IEEE Ethically Aligned Design

"

- Preserving human rights in AI systems
- Ensuring transparency and accountability in AI decision-making
- Implementing privacy-by-design principles

"

(IEEE 2024, pp. 2-5)

INDUSTRY-SPECIFIC STANDARDS

ISO/IEC 27001:2022

"

- Conducting risk assessment and management
- Implementing information security controls
- Establishing continuous improvement processes

"

(ISO 2022)

Learning Tools Interoperability (LTI) Standards

"

- Ensuring secure integration with existing learning management systems
- Enabling data portability and interoperability

"

(IMS 2024)

Web Content Accessibility Guidelines (WCAG) 2.2

"

- Ensuring the chatbot interface is perceivable, operable, understandable, and robust
- Maintaining compatibility with assistive technologies

"

(W3C 2024)

ETHICAL AI FRAMEWORKS

UNESCO Recommendation on the Ethics of Artificial Intelligence

"

- Protecting human rights and fundamental freedoms
- Promoting diversity and inclusiveness in AI systems
- Ensuring transparency and explainability of AI decisions

"

(UNESCO 2021)

OECD AI Principles

"

- Ensuring AI benefits people and the planet
- Designing AI systems that respect the rule of law, human rights, democratic values, and diversity

"

(OECD 2024)

EU Ethics Guidelines for Trustworthy AI

"

- Implementing human agency and oversight in AI systems
- Ensuring technical robustness and safety
- Maintaining privacy and data governance

"

(EC 2024)

CONTINUOUS COMPLIANCE/ONGOING AUDITING IN PERPETUITY

Regular Compliance Audits

"

- Performing annual data protection audits
- Engaging third-party security assessments

"

(ICO 2024)

Continuous Professional Development

"

- Providing regular training on evolving legal and ethical standards
- Obtaining certification in AI ethics for key personnel

"

(CIPD 2024)

References

A29WP (2018). *Guidelines on consent under Regulation 2016/679*. URL: https://ec.europa.eu/newsroom/article29/items/623051 (visited on 04/10/2024).

ACM (2024a). *ACM Code of Ethics and Professional Conduct*. URL: https://www.acm.org/binaries/content/assets/about/acm-code-of-ethics-and-professional-conduct.pdf (visited on 10/04/2024).

— (2024b). "Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency". In: New York: ACM.

Anastasiou, et al. (2024). *Translating Vital Information: Localisation, Internationalisation, and Globalisation*. Routledge.

Annus (2024). "Chatbots in Education – the impact of Artificial Intelligence based ChatGPT on Teachers and Students". In: *International Journal of Advanced Natural Sciences and Engineering Researches* 7.4, pp. 366–370.

APA (2024). *Guidelines for the practice of telepsychology*. URL: https://www.apa.org/practice/guidelines/telepsychology (visited on 04/10/2024).

Armstrong (2024). *Neurodiversity in the Classroom: Strength-Based Strategies to Help Students with Special Needs Succeed in School and Life*. ASCD.

Arrieta, et al. (2022). "Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI". In: *Information Fusion* 58, pp. 82–115.

Barocas, et al. (2021). *Fairness and Machine Learning: Limitations and Opportunities*. URL: https://fairmlbook.org/ (visited on 04/10/2024).

BCS (2024). *Code of Conduct for BCS Members*. URL: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/ (visited on 04/10/2024).

Beasley (2024). *Practical Web Analytics for User Experience: How Analytics Can Help You Understand Your Users*. 2nd ed. Morgan Kaufmann.

Bickmore, et al. (2021). "Patient and consumer safety risks when using conversational assistants for medical information: an observational study of Siri, Alexa, and Google Assistant". In: *Journal of Medical Internet Research* 20.9, e11510.

Blundell (2020). *Computer Ethics and Professional Responsibility*. Oxford, UK: Oxford University Press.

Bradbury (2024). *Successful Presentation Skills*. 6th ed. Kogan Page.

Brignull (2024). *Dark Patterns: Inside the interfaces designed to trick you*. URL: https://www.darkpatterns.org/ (visited on 04/10/2024).

CIPD (2024). *Continuing Professional Development: Guidelines and Best Practices*. URL: https://www.cipd.co.uk/knowledge/fundamentals/people/development/continuing-professional-development-factsheet (visited on 04/10/2024).

DfE (2024a). *Keeping Children Safe in Education: Statutory guidance for schools and colleges*. URL: https://www.gov.uk/government/publications/keeping-children-safe-in-education--2 (visited on 04/10/2024).

— (2024b). *Special Educational Needs and Disability Code of Practice: 0 to 25 years*. URL: https://www.gov.uk/government/publications/send-code-of-practice-0-to-25 (visited on 04/10/2024).

Dillenbourg (2024). *Artificial Intelligence in Education: Promises and Challenges*. Cambridge, UK: Cambridge University Press.

EC (2024). *Ethics Guidelines for Trustworthy AI*. URL: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai (visited on 04/10/2024).

Emam, et al. (2024). *Anonymizing Health Data: Case Studies and Methods to Get You Started*. 2nd ed. O'Reilly Media.

EU (2016). *General Data Protection Regulation (GDPR)*. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (visited on 04/10/2024).

Floridi, et al. (2024). "A Unified Framework of Five Principles for AI in Society". In: *Harvard Data Science Review* 1.1.

FTC (2024). *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*. URL: https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance (visited on 04/10/2024).

Goodman, et al. (2024). *Observing the User Experience: A Practitioner's Guide to User Research*. 3rd ed. Morgan Kaufmann.

Harper, et al. (2024). *Web Accessibility: A Foundation for Research*. 3rd ed. Springer.

Hartzog (2024). *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Harvard University Press.

Holtzblatt, et al. (2024). *Contextual Design: Design for Life*. 3rd ed. Morgan Kaufmann.

ICO (2024). *Data protection guidance*. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/ (visited on 04/10/2024).

IEEE (2024). *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems*. URL: https://standards.ieee.org/industry-connections/ec/autonomous-systems/ (visited on 04/10/2024).

IMS (2024). *Learning Tools Interoperability (LTI) Standards*. URL: https://www.imsglobal.org/activity/learning-tools-interoperability (visited on 04/10/2024).

ISO (2022). *ISO/IEC 27001:2022 Information security management systems — Requirements*. International Standard ISO/IEC 27001:2022. Geneva, Switzerland: ISO.

Josuttis (2024). *Cloud Native Transformation: Practical Patterns for Innovation*. Addison-Wesley Professional.

Jurafsky, et al. (2024). *Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition*. 3rd ed. Upper Saddle River, NJ: Prentice Hall.

Liu (2024). *Sentiment Analysis: Mining Opinions, Sentiments, and Emotions*. 2nd ed. Cambridge University Press.

Mehrabi, et al. (2024). "A survey on bias and fairness in machine learning". In: *ACM Computing Surveys* 54.6, pp. 1–35.

Miner, et al. (2022). "Key considerations for incorporating conversational AI in psychotherapy". In: *Frontiers in Psychiatry* 10, p. 746.

OECD (2024). *OECD Principles on Artificial Intelligence*. URL: https://www.oecd.org/going-digital/ai/principles/ (visited on 04/10/2024).

Quarteroni, et al. (2024). "Chatbot Evaluation Metrics: State of the Art and Future Directions". In: *Dialogue & Discourse* 12.1, pp. 1–32.

Stallings (2024). *Cryptography and Network Security: Principles and Practice*. 8th ed. Pearson.

UKGov (2008). *Education and Skills Act 2008*. URL: https://www.legislation.gov.uk/ukpga/2008/25/contents (visited on 04/10/2024).

— (2018). *Data Protection Act 2018*. URL: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (visited on 04/10/2024).

UNESCO (2021). *Recommendation on the Ethics of Artificial Intelligence*. URL: https://en.unesco.org/artificial-intelligence/ethics (visited on 04/10/2024).

Vadapalli (2024). *DevOps and Site Reliability Engineering (SRE) Handbook: Guide to Site Reliability Engineering and DevOps Practices*. Packt Publishing.

Vaughan (2024). *Human-in-the-Loop Machine Learning: Active learning and annotation for human-centered AI*. Manning Publications.

W3C (2024). *Web Content Accessibility Guidelines (WCAG) 2.2*. URL: https://www.w3.org/TR/WCAG22/ (visited on 04/10/2024).

Williams (2024). *Stand Out of Our Light: Freedom and Resistance in the Attention Economy*. Cambridge University Press.

Yesilada, et al. (2024). "How much does web accessibility cost?" In: *Proceedings of the 20th International Conference on World Wide Web*, pp. 1–10.