Exploring the relevance of Information Security policies within UK schools: A practitioner perspective

Martin Sparrius

Institute of Criminal Justice Studies, University of Portsmouth, Portsmouth, United Kingdom

Abstract

The quality of teaching and the level of student engagement within a school are acknowledged as having a significant impact on student performance. Current research into best pedagogical practices highlights how the implementation of Information Communication Technology (ICT) could potentially contribute to improved interaction by students with teaching and learning resources. It has, however been noted that ICT adoption by teachers remains below expected levels and concerns have been raised over teacher reluctance to embrace new technologies. In addition, very little research has been conducted to examine how national and school policies may hinder the pace of ICT adoption within UK schools. The lockdown of UK schools due to COVID-19 and the subsequent push to rapidly integrate more ICT for the use of remote learning has highlighted the pivotal role of a school's Information Security (IS) policy in ICT adoption. These policies and the managers responsible for interpreting them may come into conflict with teachers who want a rapid roll-out of new ICT teaching and learning tools. This paper discusses 2 examples where this conflict occurred. It argues that investigating the interactions that occurred during this period will facilitate discussion on the role IS policies have in hindering or facilitating ICT adoption within UK schools.

Keywords

Information Security, Security Policy, Schools, COVID-19, Remote Learning, Innovative Pedagogy

1. Introduction

It is largely agreed that the quality of teaching in secondary schools has a strong impact on student performance [1] and while there is discussion on the nature of this teaching, the centrality of pupil engagement and interaction is also widely recognised [2]. As the digital medium becomes more pervasive in society, and consequently schools, the discussion has shifted to the role that Information and Communication Technology (ICT) has to play in supporting this engagement and interaction [3]. Both the increasing prevalence of students possessing laptops [4] and the widespread mobile phone usage amongst students [5] emphasises how students' interaction with education and learning is changing, with students increasingly becoming digital natives who have grown up with digital technologies. This digital competence has been contrasted against teacher adoption of ICT where prior research into ICT adoption within the classroom has identified a reluctance amongst teachers to integrate ICT in their pedagogical practice [6]. Pelgrum's [7] research into this reluctance highlighted that ambivalent attitudes towards ICT and minimal computer experience amongst educators resulted in poor integration of ICT within the classroom and led to a diminishment in student engagement and progress. However, as Tondeur *et al.* [8] pointed out, the focus in prior research is more on blaming individuals and ignores the complex nature of schools. They highlighted that there is a research gap in investigating the interaction between national policies (macro-level), school policies (meso-level) and teacher (micro-level) integration of ICT within the classroom.

Proceedings of the 6th International Workshop on Socio-Technical Perspective in IS Development (STPIS 2020), June 8-9, 2020, Grenoble, France

EMAIL: martin.sparrius@port.ac.uk
ORCID: 0000-0001-8586-6767

Vanderlinde *et al.* [9] noted in their examination of ICT policy creation to promote ICT usage in Flemish schools that there was substantial variation in the philosophy of ICT policy creation between schools. Some schools practiced an inclusive discussion-based format while others employed a hierarchical approach, with teachers having no participation in decision making. They suggested that the different approaches to policy creation impacted the uptake of ICT amongst the teaching staff and echoed other research about the need for further work on the impact of ICT policy creation within schools.

The inclusion of ICT within the learning environment is largely regarded as a positive step forward in increasing student engagement and achievement; however, this greater dependence on ICT to support and deliver learning activities has increased the vulnerability of schools to various security threats. Successive Cyber Security breach surveys conducted in the UK [10]–[12] have noted the increasing risk towards UK educational organisations and this has led to the UK government conducting its first Cyber Security Breach survey focused on UK schools [13]. This survey found that approximately 79% of UK schools had reported a data breach in 2019 with nearly 25% of these incidents involving spyware or malware that was installed on the school's IT system. This concern about Information Security (IS) has been communicated to organisations in the UK [14] and consequently schools have invested in and implemented IS policies to protect critical data and processes. Research in other fields where this improvement in security has occurred has, however, found that there is potential to create security weaknesses when local work systems are ignored during the design of security frameworks [14]. It has also been highlighted that employees and security managers may have different interpretations of their organisation's policies and that this can lead to the failure of these policies [15].

This paper argues that effective involvement of teachers in the design of security policies would potentially result in better understanding of the role and application of security functions in situated practices. Using this research as a foundation while examining IS and associated ICT policies has the potential to develop our understanding of how to improve school Information Security while still encouraging best pedagogical practice.

2. An examination of Information Security policies within UK schools

There is a substantial variety of schools within the United Kingdom's education sector, ranging from independent schools, with minimal government oversight, to community schools, with substantial county council and government oversight. Correspondingly, the nature of regulatory compliance varies between schools depending on the personnel and authority in charge of the school. Additionally, within the UK there is no regulatory requirement for schools to possess an IS policy, though it is encouraged as good practice by the government's cyber security initiative [16].There is, however, a requirement for schools to possess Child Safeguarding, General Data Protection Regulation (GDPR) and Anti-terrorism (Prevent) policies [17], each of which has a significant digital component. Schools must also comply with criminal legislation, such the Computer Misuse Act (1990), when considering their IS policy. An additional consideration amongst schools is to ensure the protection of their ICT assets and it is quite probable that this concern feeds into the creation of an IS policy by a school. These factors result in a broad range in the focus, quality and presence of IS policies within UK schools.

To investigate the characteristics of these IS policies, the author collected and analysed IS policies from 100 UK schools. This analysis consisted of both quantitative and qualitative elements investigating the content, structure, school characteristics and readability of these policies.

During this initial investigation, it was observed that where schools possessed an IS policy there was substantial incorporation or reference to Safeguarding, GDPR or Computer Misuse Act (1990) content in the policy, as shown in Table 1.

Table 1
Percentage of school IS policies which contained stipulated content

	Percentage of IS policies containing stipulated content
Referred to any regulatory policy	88%
Referred to GDPR or Data Protection	77%
Referred to E-Safety or Safeguarding	31%
Referred to the Computer Misuse Act	36%

The school IS policies were also heavily negative in tone, with a substantial focus on highlighting behaviours and actions which were forbidden, with little explanation of the reasoning. 66% of the inspected IS policies stipulated software restrictions regarding the use and installation of software. The following instructions illustrate the content of many of the IS policies:

“You are not entitled to install any software of your own without the approval of the Assistant Headteacher.”

“Staff must not use, download or install any software, app, programme, or service without permission from Network Team”

“An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users - no programmes are to be installed without the knowledge of the Headteacher and the e-safety lead”

This initial analysis suggests that the dominant motivation when creating these IS policies is regulatory compliance and asset protection, rather than pedagogical best practice. Creation of these policies was very likely to have centred around the input from the IT manager, Safeguarding personnel and the Data Protection officer for the school. In UK schools, these positions are associated with support staff or senior management and not classroom teachers, whose input would have been limited in scope. Hence, it becomes apparent that the use and incorporation of ICT within the classroom is significantly influenced by the IT manager. Teachers, in contrast, face penalties, up to dismissal from employment, for violating the school’s IS policy.

In addition the poor accessibility of IS policies has been highlighted by Weidman and Grossklags [18], who identified how poor readability and long policy length acted as an hinderance to staff engaging with their organisation’s IS policy. Prior analysis by the author [19] of the readability of 100 UK schools’ IS policies was conducted using the Flesch Reading Ease and Simple Measure of Gobbledygook (SMOG) scales and found that many UK schools’ IS policies had an average or higher readability difficulty (Table 2).

Table 2
Readability analysis of school IS policies

	Recommend value	Mean Value	Standard Deviation	Minimum	Maximum

Flesch Reading Ease	Greater than 40	42.7	7.9	18.1	65.2
SMOG	Less than 13	12.9	1.43	10.1	15.5
Word Count		3962	3327	424	20352

This inaccessibility would act as a hindering factor in a teacher's attempts to understand the relevance and purpose of their schools' IS policy. Additionally, it puts the IT manager, who presumably has a greater understanding of the policy, in the position of being a gatekeeper to understanding and interpreting the policy content.

Overall, the above factors create an environment where teachers are highly dependent on the IT/school manager's approval of ICT requests based on their judgment that such requests do not violate the school's IS policy, rather than on pedagogical grounds. Despite this, incremental improvements to teaching practices that involved ICT have still been noted [20]. However, this is likely due to any requested changes being limited in scope and discussed over a period of time with school managers before eventual trial and adoption within the classroom.

3. COVID-19 and a changed education landscape

This status quo was disrupted by the outbreak of COVID-19. The changes that were forced on schools because of the outbreak exacerbated the tension between school employees and ICT managers. The disconnect between those who create policies and those who must implement them became more apparent as innovation in developing remote schooling was demanded of the teaching staff. By 26th of March 2020, all UK schools were ordered to close their premises [21] with substantial confusion resulting as it was unclear if the closures were temporary or whether they would last until the end of the school year. Consequently, the response from schools was varied, with some schools planning for home working for the rest of the year and other schools planning for short term stop gaps until a return to school premises. This unfamiliar territory presented teachers with a situation where they needed to transfer much of their teaching online, creating an environment where there was a potential for a clash between the needs and desires of the teacher to plan and execute lessons and the restrictive nature of schools' IS policies that required permissions and checks.

This potential conflict is unsurprising for researchers within socio-technical theory. In 2006 Mumford [22] had already recognised that as the working environment moved away from a traditional workplace to a more fluid digital environment, employer-employee interactions would also need to change as what worked previously could instead lead to alienated and disaffected employees. Socio-technical theory has also highlighted that when Information Security practices are not integrated with working activities, staff will act to ignore or circumnavigate these practices to perform their job [23]. The pace of events during the Covid-19 crisis has served to highlight how a lack of involvement of staff who are essential to the core role of an organisation can handicap effective working and this becomes particularly apparent in situations where quick decision making is required.

These problems were very evident within schools as discussion moved to how good pedagogical practice could be maintained by having interactive lessons when students and staff were based away from the school site. Green [24] found substantial variation in the extent and nature of work undertaken by UK students during this time of remote learning. One fifth of students did less than an hour a day and only 17% did over 4 hours, with many completing schoolwork that consisted solely of worksheets and watching videos. As the lockdown continued, there was persistent discussion in the media about the quality of education provided to students isolating at home [25]; however, there was relatively little discussion about the IS considerations that teachers needed to account for in their lesson delivery.

In contrast, substantial debate was occurring within the teaching profession over the pedagogical and IS merits and flaws of various virtual learning spaces, with some raising concerns over safeguarding [26], while others viewing the crisis as an opportunity to reinvent lesson delivery [27]. Solutions that were offered ranged from simplistic and secure PowerPoint document storage to fully active virtual classrooms. Two examples from the author's observations in a UK college during this period are presented as exemplars of this situation.

3.1. Example 1: Conducting virtual lessons

Google Meet, Microsoft Teams and Zoom have all been advertised as virtual learning spaces where students can benefit from improved engagement by being able to interact with their teacher and each other in real time. As Google usage is extensive within UK schools, Google Meet was available from the beginning of the lockdown as a tool for virtual meetings and was the initial virtual learning space for many schools. Prior to the lockdown, there was limited use of Google Meet in a classroom setting, as there was very little need for virtual meeting software pre-COVID-19, and the author's analysis of school IS policies highlighted that few schools had considered the implications of the widespread usage of this software. As the lockdown progressed, teachers started requesting access and use of Google Meet to conduct online lessons. Safeguarding concerns around webcam usage were immediately raised regarding teachers having virtual access to students' private household space and contrasted against concern that the lack of video would lead to student disengagement from the lesson. In the author's college, student webcam usage was banned on the recommendation of the IT manager until the end of the lockdown and some teachers resorted to different strategies, such as a verbal 'sound off' every 15 minutes, to check if students were still present. Access to Microsoft Teams and Zoom, with their improved functionality, was denied due to security concerns and restricted to staff usage, though it was noted that other schools in the area were using Microsoft Teams to conduct online teaching. This highlighted the centrality of the school's IT manager, rather than the school's teachers, in deciding what was appropriate as a tool for classroom learning.

3.2. Example 2: Barriers to innovative teaching

Pre-recording of lessons and the use of PowerPoints became the default approach for many UK teachers during the lockdown and many schools used Google Classroom or similar virtual learning environments to distribute these resources. Current good pedagogical practice recognises that students experience more meaningful learning when interacting with their education materials and passive absorption via video or written material is less effective[3]. As the lockdown progressed it was noted that an increasing number of apps were available via Google's App store that provided interactive quizzes, crossword puzzles and other activities. App installation via the App store is restricted within most schools and their installation prohibited by most schools' IS policies. At the author's college, requests for temporary installation rights were denied by the IT manager as it was deemed too much of a risk of malware being installed to allow teachers to install software individually. However central installation was never offered as an alternative. Generally, the message from the IT manager was 'what we have works' and that IS and Safeguarding were more important than good pedagogy during this period.

With limited guidance from the government during the lockdown, schools were forced to make their own decisions about the appropriateness of each piece of software. Based on the author's reading of the school IS policies from around the UK, it is highly likely that platform and software use decisions would have rested with the IT manager and not members of the teaching staff. As demonstrated by the scenarios above, these centralised actions are likely to have resulted in decision making that erred on the side of security instead of usability and promoting good pedagogical practice. They also demonstrate the limited usefulness of several existing security policies in providing proactive measures to cope and tackle uncertain risks such as those posed by Covid-19.

4. Conclusion

The UK educational landscape continues to face an uncertain future with potential waves of COVID-19 infection likely to disrupt any attempts for schools to return to normal operation in the foreseeable future. The use of IT to provide digital delivery of content for students that are quarantining or for schools in lockdown will continue to be of importance. Short term solutions revolving around maintaining the old status quo are increasingly unviable as both schools and teachers look to adapt to a tumultuous environment where IT plays an increasingly central role in content delivery. This situation will continue to exacerbate the tension between IT security concerns and digital pedagogical practice. The author acknowledges that ultimately for most organisations security will be the central concern, but by potentially marginalizing teachers' pedagogical concerns this can create a situation where these teachers seek to work around, rather than with, their IT departments. There needs to be a focus on how best to manage this situation so that feedback from all the stakeholders is accounted for and a new system that incorporate both IS and pedagogical objectives is created.

To explore this further the author proposes to interview secondary school teachers to capture firsthand their IT experiences during the COVID-19 period: how they interacted with their IT departments and their thoughts on the tension between IS and the freedom to adapt their teaching practice. Based on this research, the author plans to explore whether school IS policies acted to constrain and hinder good pedagogical practice or if the IS systems were flexible enough to incorporate staff feedback and demands.

5. References

[1] M. Barber and M. Mourshed, *How the world's best performing schools systems come out top*. McKinsey & Company, 2007.

[2] C. Husbands and J. Pearce, "What makes great pedagogy ? Nine claims from research Chris Husbands and Jo Pearce," 2016.

[3] R. Scherer, F. Siddiq, and J. Tondeur, "Computers & Education The technology acceptance model (TAM): A meta-analytic structural equation modeling approach to explaining teachers ' adoption of digital technology in education," *Comput. Educ.*, vol. 128, no. 0317, pp. 13–35, 2019.

[4] L. R. Elliott-dorans, "Computers & Education To ban or not to ban ? The e ff ect of permissive versus restrictive laptop policies on student outcomes and teaching evaluations," *Comput. Educ.*, vol. 126, no. July, pp. 183–200, 2018.

[5] H. Crompton and D. Burke, "Computers & Education The use of mobile learning in higher education : A systematic review," *Comput. Educ.*, vol. 123, no. April, pp. 53–64, 2018.

[6] B. Berrett, J. Murphy, and J. Sullivan, "Administrator insights and reflections: Technology integration in schools," *Qual. Rep.*, vol. 17, no. 1, pp. 200–221, 2012.

[7] W. J. Pelgrum, "Obstacles to the integration of ICT in education: Results from a worldwide educational assessment," *Comput. Educ.*, vol. 37, no. 2, pp. 163–178, 2001.

[8] J. Tondeur, H. van Keer, J. van Braak, and M. Valcke, "ICT integration in the classroom: Challenging the potential of a school policy," *Comput. Educ.*, vol. 51, no. 1, pp. 212–223, 2008.

[9] R. Vanderlinde, J. Van Braak, and S. Dexter, "Computers & Education ICT policy planning in a context of curriculum reform : Disentanglement of ICT policy domains and artifacts," *Comput. Educ.*, vol. 58, no. 4, pp. 1339–1350, 2012.

[10] R. Klahr, J. N. Shah, P. Sheriffs, T. Rossington, and G. Pestell, "Cyber Security Breaches Survey 2017: Main report," *UK Gov.*, no. April, pp. 1–66, 2017.

[11] C. Department for Digital, "Cyber Security Breaches Survey 2018," 2018.

[12] M. and S. Department for Digital, Culture, "Cyber Security Breaches Survey 2019," 2019.

[13] M. & S. Department for Digitial, Culture, "Cyber Security Breaches Survey 2020 - Education Annex," 2020.

[14] M. Sadok, S. Alter, and P. Bednar, "It is not my job: exploring the disconnect between

corporate security policies and actual security practices in SMEs," *Inf. Comput. Secur.*, vol. 28, no. 3, pp. 467–483, 2020.

[15] S. Samonas and G. Dhillon, "Stakeholder perceptions of information security policy : Analyzing personal constructs," *Int. J. Inf. Manage.*, vol. 50, no. April 2018, pp. 144–154, 2020.

[16] "Small & medium sized organisations - NCSC.GOV.UK." [Online]. Available: https://www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations#section_4. [Accessed: 19-Sep-2020].

[17] Department for Education, "Statutory policies for schools and academy trusts," *Statutory policies for schools and academy trusts*. [Online]. Available: https://www.gov.uk/government/publications/statutory-policies-for-schools-and-academy-trusts/statutory-policies-for-schools-and-academy-trusts.

[18] J. Weidman and J. Grossklags, "What's in your policy? An analysis of the current state of information security policies in academic institutions," *26th Eur. Conf. Inf. Syst. Beyond Digit. - Facet. Socio-Technical Chang. ECIS 2018*, pp. 1–16, 2018.

[19] M. Sparrius, "An analysis of United Kingdom School's Information Policies: A socio-technical approach," in *STPIS 2020: Socio-Technical Perspective in IS Development 2020*, 2020.

[20] G. Sang, M. Valcke, J. V. A. N. Braak, and J. Tondeur, "Factors support or prevent teachers from.pdf," in *Proceedings of the 17th International Conference on Computers in Education [CDROM].*, 2009, pp. 808–815.

[21] Department for Education, "Guidance for schools, childcare providers, colleges and local authorities in England on maintaining educational provision - GOV.UK." [Online]. Available: https://web.archive.org/web/20200320152139/https://www.gov.uk/government/publications/coronavirus-covid-19-maintaining-educational-provision/guidance-for-schools-colleges-and-local-authorities-on-maintaining-educational-provision. [Accessed: 29-Oct-2020].

[22] E. Mumford, "The story of socio-technical design: Reflections on its successes, failures and potential," *Inf. Syst. J.*, vol. 16, no. 4, pp. 317–342, 2006.

[23] P. Bednar and V. Katos, "Addressing The Human Factor In Information Systems Security," *MCIS 2009 Proc.*, 2009.

[24] F. Green, "Schoolwork in lockdown : new evidence on the epidemic of educational poverty . Professor of Work and Education Economics , UCL Institute of Education . Executive Summary .," 2020.

[25] K. Sellgren, "Coronavirus: A third of pupils 'not engaging with work' - BBC News," *BBC News family and education corresponden*, 2020.

[26] A. Gibbons, "Coronavirus: 10 safeguarding rules for teachers at home | Tes," *TES*, 2020. [Online]. Available: https://www.tes.com/news/coronavirus-10-safeguarding-rules-teachers-home. [Accessed: 19-Sep-2020].

[27] G. Tam and D. El-Azar, "3 ways the coronavirus pandemic could reshape education | World Economic Forum," *World Economic Forum*, 2020. [Online]. Available: https://www.weforum.org/agenda/2020/03/3-ways-coronavirus-is-reshaping-education-and-what-changes-might-be-here-to-stay/. [Accessed: 19-Sep-2020].