Slide 1: Title of research: Utilising and adapting IoT technology in secondary education

Utilising and adapting of internet and IoT devices in secondary education becomes essential nowadays. Students have their own laptop or chromebook, for their studies; teachers are using cloud technologies to deliver a lesson. For example, Google Classroom, Microsoft One-Note, instead of traditional way of teaching, with blackboard or whiteboard; schools also use IoT to keep tracking every student's performance, both academic and behaviour; registers are done online with smartcard: not only can track whether they have arrived school on time everyday, but also can trace what facilities they have accessed always in school.

Besides the students management, IoT devices and technologies are also playing a major role on the security of schools. For example, CCTV, smart alarms and automatic school gate control.

The topic is to research the secondary schools able to utilise the IoT devices and technologies, and how; besides the benefits, the study also research the impacts to students and staffs, when a school is fully adpating and utilising IoT on every aspect.

Slide 2: Significance of the research:

IoT is widely used in secondary education, teaching, student and class management, and school security.
IoT can deliver teaching materials interactively, track the performance data of every student, which helps teachers to simplify the process and workload; teachers no need to count every student attendence as they have smartcard to enter the school, the time and where have they been are also recorded; SEN students' data can be stored on cloud and be assessd by SEN teachers or social workers easily and provide the best support to these students.
Although IoT has given schools efficiencies and benefits, impacts are created simultaneously to both students and teachers, including privacies, personal data exposure and the possibility of violations with laws and regulations. For example, the tracking data of students should be stored and accessed, comply with the latest regulations. For example, GPDR and DSS (DfE, 2018).

Slide 3: Research question:

IoT is widely used in secondary education, do the students and teachers understand how to use it correctly? While they enjoy the benefits of IoT devices and technologies, do they know how to minimise the impact, such as privacy and personal data security.

Slide 4: Aims and Objectives:

- To identify the most popular IoT devices or technologies utilised in secondary institutions. This is including any IoT of school and students' management, students' performance management, SEN management, delivery of lesson and schools' security.

- To identify the benefits of utilising IoT in secondary schools, from the quality of teaching to school management. For example, the increase of efficiency, easier and centralised management, students' performance tracking, quicker recongition of student needs, such as the SEN; more effective repsonse of the premises' security and tracking of the schools' properties.
- To identify the impact of IoT utilisation, including the privacies and potential violations of the laws and regulations. The most common is the privacy, including the students' personal information and medical information. GPDR and HIPAA are involved in this case.
- A short survey will be conducted to research IoT utilisations and their impacts. Targets will be the school teachers and students. Questions are including:

  1. Do they use IoT in school. For example, smartphones, tablets, computers, smartcards, etc.

  2. Which kind of IoT do they use the most

  3. Do they need to log in when accessing their IoT devices or websites

  4. Will they share the IoT devices with others

  5. Will the IoT for their personal use. For example, access their personal social media and email accounts.

  6.How long will they change their password

  7. Will they reuse their previous passwords

  8. Will they use the same password in both personal and school accounts

  9. Will they store the school accounts passwords into their personal computers

  10. Will they share the password with others.

  11. Will they lock or shutdown their laptop/tablet after use.

12. Any regulation or compliance policy they need to follow when accessing student's information (For staff only).

13. Do they think they have followed the compliance policy strictly (For staff only).

14. Do they have their own login when accessing any student information (For staff only).

15. How do they store the data, any encryption (For staff only) (Senthilkumar, Kavitha & V E., 2017).

Slide 5: Literature related to the project:

1. Canbaz, A., OHearon, K., McKee, M. and Hossain, M. (2022). IoT Privacy and Security in Teaching Institutions: Inside The Classroom and Beyond. 2021 ASEE Annual Conference, [online] (33905), p.2-4. Available at: https://strategy.asee.org/iot-privacy-and-security-inteaching-institutions-inside-the-classroom-and-beyond.pdf [Accessed 10 Feb. 2022].

2. Alexei, Arina & Alexei, Anatolie. (2021). Analysis of IoT security issues used in Higher Education Institutions. International Journal of Mathematics and Computer Applications Research. 9. 2277-2286. 10.47191/ijmcr/v9i5.01.

3. A. Jaklié, "Educating the Educators for Introducing Internet of Things to Primary and Secondary Schools' Curriculums," 2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO), 2020, pp. 632-635, doi: 10.23919/MIPRO48935.2020.9245223.

4. Francisti, J., Balogh, Z., Reichel, J., Magdin, M., Koprda, Š. and Molnár, G., 2020. Application Experiences Using IoT Devices in Education. Applied Sciences, [online] 10(20), p.7286. https://doi.org/10.3390/app10207286.

5. Mishra, Aryan & Karthikeyan, J. & Barman, Binoy & Veettil, Roy. (2020). Journal of Critical Reviews REVIEW ON IOT IN ENHANCING EFFICIENCY AMONG HIGHER EDUCATION INSTITUTIONS. 10.31838/jcr.07.01.109.

6. BAGHERI, Maryam and HAGHIGHI MOVAHED, Siavosh (2017). The Effect of the Internet of Things (IoT) on Education Business Model. In: 2016 12th International Conference on SignalImage Technology & Internet-Based Systems (SITIS). IEEE Computer Society, 435-441.

7. Sha, K., Wei, W., Andrew Yang, T., Wang, Z. and Shi, W. (2018). On security challenges and open issues in Internet of Things. Future Generation Computer Systems, 83, pp.326–337.
8. Park, M., Oh, H., & Lee, K. (2019). Security Risk Measurement for Information Leakage in IoTBased Smart Homes from a Situational Awareness Perspective. Sensors (Basel, Switzerland), 19(9), 2148. https://doi.org/10.3390/s19092148

9. Tomás, Cecília & Teixeira, Antonio. (2020). Ethical Challenges in the Use of Iot in Education: On the Path to Personalization. EDEN Conference Proceedings. 217-226. 10.38069/edenconf-2020-rw-0024.

10. Garg, R. (2018). Open data privacy and security policy issues and its influence on embracing the Internet of Things. First Monday, 22(5).

11. Office of the Victorian Information Commissioner. (2021.). Internet of Things and Privacy -Issues and Challenges. [online] Available at: https://ovic.vic.gov.au/privacy/internet-ofthings-and-privacy-issues-and-challenges/

12. Data protection: a toolkit for schools Open Beta: Version 1.0. (2018). [online] Available at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747620/Data_Protection_Toolkit_for_Schools_OpenBeta.pdf

Slide 6: Research Design:

1. Case studies: To identify what IoT devices and technologies are widely used in secondary institutions.
2. Questionnaire: The audience will be the students and staff in secondary schools. Questions include the use of IoT, their behaviour when using it, any security awareness to these devices, etc (Senthilkumar, Kavitha & V E., 2017).

Slide 7: Ethical considerations and risk assessment:

Questionnaire: As a questionnaire may need to collect any personal information. In the first question, I will ask the audience if they are happy to participate in the survey and declare that all data will be only used for the research. All data will be deleted after the study is completed.

A consent statement will be added before the start of the questionnaire to make sure the questionnaire is compliant with the privacy laws and regulations.

The consent statement will be like the following:
“Do you agree to the above terms? By clicking Yes, you consent that you are willing to answer the questions in this survey.”

“Do you consent to your personal data being processed as described above? You must click Yes in order to take the survey.” (Surveymonkey, 2022)

This is important because I need to comply with the current regulation, especially the GPDR. According the GPDR Article 6(1) (i-scoop, 2022), controllers, who are processing the data, must have a lawful basis for the processing activity, which are the answers I will collect in the surveys. I need to make a consent for the participents, to inform them all data will be processed lawfully, transparent, fair, accurate, accountable, with integrity and confidentity, also have limitation on purpose and storge.

Slide 8: Artefacts that will be created:

1. Data from the questionnaires – which are the answers and responses from the audience in the questionaires.
2. Questionnaire analysis. For example, the behaviour of using IoT, awareness of cyber security, etc. This will be part of the quantitative research: the numerical data will become statistics, to analyse and interpret the statistics and get a conclusion (Kirsty and Graeme, 2018).
3. The study's outcome: Levels of IoT utilisations in secondary education institutions and their impact of cybersecurity to the users.
4. Suggestions, if any. This will be qualitative research, which means I will collect non-numerical data, such as comments, opinions, and experiences. In this case, gather in-depth insight into the cyber security-related problem of using IoT, and recommend any solution on the research.

Slide 9: Timeline of proposed activities:

1. Create and desgin questionnaire (1 week)
2. Check the questions of the questionnaire (1 week)
3. Publish the questionnaire, advertise to education agents, secondary students and staff to participate (2 weeks)
4. Collection of surveys (1 week)
5. Analysis of the data (1 week)
6. Start writing the research (2-12 weeks)

Reference:

1. help.surveymonkey.com. (2022). Adding a Consent Statement or Privacy Notice. [online] Available at: https://help.surveymonkey.com/articles/en_US/kb/How-do-I-create-a-consent-form-or-disqualify-respondents-from-a-survey.
2. Data protection: a toolkit for schools Open Beta: Version 1.0. (2018). [online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747620/Data_Protection_Toolkit_for_Schools_OpenBeta.pdf.
3. Senthilkumar, Kavitha & V E., Sathishkumar. (2017). A Survey on Cyber Security awareness among college students in Tamil Nadu. IOP Conference Series: Materials Science and Engineering. 263. 042043. 10.1088/1757-899X/263/4/042043.
4. Kirsty Williamson and Graeme Johanson (2018). Research methods : information, systems, and contexts. Cambridge, Ma Chandos Publishing.
5. Bhandari, P. (2020). An introduction to qualitative research. [online] Scribbr. Available at: https://www.scribbr.com/methodology/qualitative-research/.