- # **UK Engineering Council Guidance on Security**

Security is an important consideration for any project and in any workplace. UK SPEC provides guidance on security and outlines how it expects professional engineers to conduct themselves with respect to security. This guidance is split into six key principles. Your task is to visit the UK SPEC security page and read through the tips provided for each principle.

Using the tips on the webpage provide at least one example for each of the six principles that you can directly link to your project or that should be considered in the role of Professional Engineer. Then summarise your findings in the comments box below.

The link is https://www.engc.org.uk/security

- ## How would you adopt a security-minded approach to your project?

  - be responsive to changes in the operating environment, including the impact of changes in use of the asset or system, its wider connectivity and emerging threats and vulnerabilities. With the current situation with working from home and potential changes to the working environment, this will be relevant to how I consider security.
  - remember that security risk assessment is an aid to professional judgement, not a substitute for it. I will continue to assess any and all security risks throughout the project to ensure that any risks are neutralised as quickly as possible.

- ## What should you consider in order to apply responsible judgement and take a leadership role?

  - working with other professionals to ensure informed, proportionate, holistic judgements. When I am working with other professionals – eg. When using equipment like a hyper-spectral camera – I will strive to ensure that we both are remining security minded throughout the work
  - being prepared to challenge assumptions and proposals. If when working with one of these professionals, they do something that could potentially cause a security risk, I will certainly be prepared to challenge them and stop them from presenting those risks.

- ## How will you ensure that your project complies with legislation and codes, while understanding intent and prepared to seek further improvements?

  - be aware of, and comply with, the security-related laws in countries where they operate or where their products or services will be used. As I will be developing a prototype product, I will ensure that I am aware of the relevant laws and will comply with them entirely when developing my product.
  - be open-minded and avoid using regulations to facilitate complacency. By constantly evaluating the security risks, I will ensure that I am constantly staying on the ball, and not becoming complacent.

- ## How do you ensure good security-minded communications?

  - adopt appropriate measures to protect sensitive information when it is communicated, used and stored, both within and beyond their organisation. Whenever sharing information, I will ensure that it is done in a secure way, and I will communicate when it needs to remain secure.
  - recognise the persistent nature and accessibility of information published on the internet or otherwise made publicly available. Before making any information publicly available on the internet, I will ensure to conduct a thorough review of the content and redact or not publish any sensitive information.
  - recognise that indiscriminate publication of project, technical or personal information can aid reconnaissance and enable security breaches through social media. No personal, technical or project information will be shared on social media.
  - ensure responsible use of social media use for both personal and professional purposes. I will avoid using social media for ANY professional or personal uses throughout the year.

- ## How would you go about understanding, complying with and seeking to improve lasting systems for security governance?

  - ensure that there are appropriate mechanisms for reporting and feedback on security incidents and issues. Security discussions will occur often with my supervisor to ensure that any security issues can be reported as quickly as possible.
  - contribute to the development and review of relevant security management frameworks, particularly about aspects which may not be well understood. All the security frameworks used for this project will be made by me with the specifics of this project in mind

- ## What do you need to consider when contributing to public and professional awareness of security?

  - be security-minded during public discussion. When publicly discussing the project, I will ensure not to share any sensitive information about any part of the project.
  - contribute to public and professional awareness of security by sharing and promoting knowledge of effective solutions. When I come across useful security resources, I will share them with my supervisor and ask that he can share them to more people that that resource will be relevant to.

<u>Summarise how you will address security in your project</u> *(max 200 words)*

By avoiding sharing any information about my project publicly, I will be able to reduce a large portion of the security risks involved. If I do speak about my project with others, I will make sure to only share with them information that has been labelled as safe. If it is required for me to share sensitive information with any other party, I will ensure that they are aware of the sensitivity of the data and that they have signed a form to ensure they do not share this data without my consent, which will be withheld unless the sharing of said data is strictly necessary.

As I do not plan to use human subjects in my project, I hope to minimise the amount of sensitive information that is collected for the project. However, I will still scrutinise every piece of information gathered and generated for the project to ensure that it doesn't pose a security risk.