# Ethics in Computing

As a cyber security professional in current practice, I encounter multiple ethical issues, regularly.

I must approve and deny software, and almost daily receive such requests. As I work for a relatively new and growing business, there is a lack of governance over what is approved for legacy systems. This makes it extremely difficult to do my job effectively. There is no domain, nor central deployment method to push software out from, and so this makes governance even more difficult. The business does however, have Endpoint Detection and Response (EDR) software, and it is mandatory for any device to have this installed before connecting to the corporate network or systems, and this alerts us, via an outsourced Security Operations Centre (SOC), of any suspicious or malicious binaries found on any device.

To make things more complex, the business also allows to some degree Bring Your Own Devices (BYODs) on to the network. This is an increasing trend at the company and causes anxiety.

Some malicious software found on many BYOD devices is Key Management Service (KMS) software, a type of key cracking software used to activate Microsoft products. In order to allow these devices on to the network, a decision was made to enforce such software to be removed before they were allowed to join the network due to their known association to introducing malware.

This is illegal software, however on what grounds can users who bring their own laptop in for work be ordered to remove software which they have been otherwise using based on their own ethics? Removing such software would also force them to pay for software licences that they would otherwise not have had to pay for. After all, this is for work the business is asking them to do, while not providing sufficient hardware and software to do so. This would be especially hard hitting for lower earners, and would cause conflict with several ethical principles such as point 4 of the BCS Public Interest principle (BCS, N.D.). They perhaps should be reported, although there are now strict rules to disallow them access to the network unless such software is removed. Therefore, the problem is removed from further conflict. Some users consent to this, however others do not agree and choose to continue working from a corporate device, often of a lower specification. This obviously still leaves the issue of whether the finding should be reported or not.

Another ethical dilemma is the fact that, because of the lack of governance, the security team cannot see which devices are connecting and there is currently very little to stop rogue devices from accessing systems if they have correct login credentials. So should special dispensation be given for those that volunteered their own devices so that they are known? It seems especially unfair to punish them.

Another ethical issue that arose as part of the same subject is that there was a security incident recently, and suspicion was aimed at several individuals. In order to rule them out from suspicion, it was important to find out if accountability lied with themselves, or a third party who had found a way to breach their valid credentials in order to carry out the attack. Because of this, it was pertinent to collect all suspected individuals’ workstations for forensic analysis. However, the decision was made to exclude any personal devices, and to have them forward logs instead. This was clearly to protect the users’ property, however even system logs to some degree may uncover clues as to an individual’s personal use of the machine. This concerns ethics described in point 1.6 and 1.7 of the ACM (2018) code. E.g., How much data can be taken? How long is it kept? Could something they offer up innocently actually end up causing more harm to that user? Should principle 2.8 supersede 1.6 and 1.7 of the same code? These are difficult ethical decisions and they are often made using utilitarianism-based views, where the decision is taken that causes the least harm or ill feeling (Stahl, 2016).

The use of the EDR software already raised the alert level for a large proportion of the staff, who did not like the idea of “Big Brother” watching them. As a new UK based security team, it was already somewhat difficult gaining the trust of a former Soviet staff base. Particularly as proceedings started as an “us and them” style way of working, inclusivity is now key in all operations. Members from Russian teams are included in meetings and transparency is forefront. When rolling out the EDR software, the business was completely transparent on what data the software captures, how it may affect any work, and what information can be seen. This has helped to develop smoother relations. After all, trust has to be earned, and can be lost in one simple act of deviation.

Another project introduced was the delivery of a training program used to deliver security awareness content, and more advanced training, this relates to point 2.7 of ACM’s code (ACM, 2018). The video-based cartoon like training program contains mainly characters of white ethnic origin, and so the business decided to purchase additional premium content so a wide range of minority groups could be represented. Additionally, the content was transcribed into Russian language versions, satisfying point 3.3 of the ACM code of ethics (ACM, 2018).

Even though the company is transitioning to English, the business is still aware that many of the staff base do not speak the language, and relations have to be cemented by trying to be as inclusive and fair as possible, adhering to point 3 of BCS’s Public Interest principle (BCS, N.D.).

Finally, as a Certified Information Systems Security Practitioner (CISSP) holder, I am required to earn CPD units every year, something that falls in line with point 3 of BCS’s Professional Competence and Integrity principle. Furthermore, as an active member of ISC2, I am also bound by the following ISC2 code of ethics (ISC2, N.D.):

## **Code of Ethics Preamble:**

* The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behaviour.
* Therefore, strict adherence to this Code is a condition of certification.

## **Code of Ethics Canons:**

* Protect society, the common good, necessary public trust and confidence, and the infrastructure.
* Act honourably, honestly, justly, responsibly, and legally.
* Provide diligent and competent service to principals.
* Advance and protect the profession.

**References**

Association for Computing Machinery. (2018) ACM Code of Ethics and Professional Conduct. Available from: <https://www.acm.org/code-of-ethics> [Accessed 4 October 2022].

British Computer Society. (N.D.) BCS Code of Conduct. Available from: <https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct> [Accessed 4 October 2022].

ISC2. (N.D.) (ISC)2 Code of Ethics. Available from: <https://www.isc2.org/Ethics> [Accessed 24 September 2022].

Stahl, B. C., Timmermans, J. & Mittelstadt, B. D. (2016) The Ethics of Computing: A Survey of the Computing-Oriented Literature. [*ACM Computing Surveys*](https://dl-acm-org.uniessexlib.idm.oclc.org/toc/csur/2016/48/4) 48(55): 1-38. DOI: https://doi-org.uniessexlib.idm.oclc.org/10.1145/2871196