Tutorial 1 – Ethics and legislation in IT

In groups:

1. For you, what is the difference between the law and ethics? Discuss your views. Give a computing-related example of something legal but that might be considered unethical, and something that is illegal but might be considered ethical.
   They are definitely related. The law can be considered a form of codified ethics … a result of a societal discussion about acceptable behaviour that is then codified in the law and backed up by the police, the judiciary and other aspects of legal administration. Ethics is about what is right and wrong as the basis for how people should behave in society. Ethical viewpoints sometimes differ, but ethical discussion is part of the discourse we have in society. Because the law deals with 'crime' and 'malpractice', it covers actions that are particularly 'bad', but our ethical views can affect our actions in daily life, such as how we interact with others, what jobs we do, how we help others etc.
2. Find the official source of the UK Computer Misuse Act and the EU GDPR. What are these pieces of legislation designed to protect? Where are they relevant and why are they important for developers?
   Computer Misuse Act 1990 – https://www.legislation.gov.uk This is the source of all currently valid UK law. The CMA is designed to protect computing systems from being hacked, provided they have adequate defences. It is relevant throughout the UK. It is important as it criminalises unauthorised hacking and attacks (such as DOS attacks), although there have been few prosecutions. Implications for developers are that authorised access to systems needs to be clear and understood, and appropriate security measures need to be in place.
   EU GDPR – https://eur-lex.europa.eu/ Also, a good source for the law + advice is https://gdpr-info.eu/. The GDPR is designed to protect personal data from being inappropriately shared, stored or used. It is relevant throughout the EU. It is also relevant in UK law as the GDPR was retained in UK law after we left the EU. It is also relevant for any company in the world that deals with EU citizens. Implications for developers are that they need to understand what personal data is and to develop systems that comply with data protection regulations in the UK and elsewhere in the world.
3. What is the difference between criminal and civil law?
   Criminal law deals with society's offences and seeks punishment for those offences. The government prosecutes criminal cases. Civil law is for individual disputes and seeks to achieve a remedy for the injured party. Civil cases are prosecuted by private individuals.
4. What is the law of precedence? How does it work in UK law?
   The law of precedence, also called Common Law, refers to court decisions that are considered an authority for deciding subsequent cases involving identical or similar facts or similar legal issues. The UK uses common law, and the hierarchy of courts is important. A court is bound by the decisions of a court above it and, usually, by a court of equivalent standing. Superior courts have the power to overrule decisions of lower courts and, in certain cases, to overrule their own decisions.

5. What is the hierarchy of courts in the UK?
   Broadly it is like this:

6. Here is a report from a 1988 Appeal Court case that had big implications for computer law:

R v Gold & Schifreen (1988) 1 AC 1063

Robert Schifreen and Stephen Gold gained unauthorised access to British Telecom's Prestel interactive viewdata service in 1984/5 on numerous occasions. Schifreen had observed the password of a Prestel engineer at a trade show. They explored the system and accessed the personal message boxes, including that of Prince Philip. They obtained information to which they were not entitled, made unauthorised alterations to stored data and caused charges to be made to account holders without their knowledge or consent.

They were found guilty under section 1 of the Forgery and Counterfeiting Act 1981, of defrauding BT by manufacturing a "false instrument," namely the internal condition of BT's equipment after it had processed Gold's eavesdropped password.

However, the appeal court acquitted them and the Lords upheld the acquittal.

Lord David Brennan said:

"We have ... come to the conclusion that the language of the Act was not intended to apply to the situation which was shown to exist in this case. The submissions (of no case to answer) at the close of the prosecution case should have succeeded. It is a conclusion which we reach without regret. The Procrustean attempt to force these facts into the language of an Act not designed to fit them produced grave difficulties for both judge and jury which we would not wish to see repeated. The appellants' conduct amounted in essence, as already stated, to dishonestly gaining access to the relevant Prestel data bank by a trick. That is not a criminal offence. If it is thought desirable to make it so, that is a matter for the legislature rather than the courts."

a. Why was the password they used not a 'false instrument'?
   A password is not an 'instrument' that can be 'manufactured' in the same way that a physical key or card is. In this case, it wasn't 'false' either – the hackers had the correct password.

b. Do you think this was the correct decision? Why?
   Yes, because there was no forgery involved. At the time of this case, there was no legislation that criminalised hacking if hackers had the correct password. The invisibility of computing meant that physical keys and protections were no longer effective – this created a 'policy vacuum'.

c. What were the implications of this decision? What would happen now?
   Ultimately, it resulted in the creation of the Criminal Misuse Act. The hacking took place in 1984/5 but the CMA didn't come into force until 1990, so there was a long period during which there was no adequate legislation for hacking offences. The lag in writing appropriate tech-related law is still a problem. If this happened now, Gold & Schifreen could be prosecuted under the CMA.