Lesson plan

|  |
| --- |
| Topic 3 Current legislation |
| Learning Objectives:   * Describe the role of current legislation (and subsequent additions and amendments) in protecting users and their data from attack or misuse   This topic covers the role of current legislation in protecting users and their data in F2. The moral and ethical factors are covered in Topic 4. |
| Content |
| Starter  PowerPoint guide: Topic 3 Current legislation.pptx  Have any of the students watched the TV series ‘Humans’? This is a sci-fi series about robots or ‘synths’, created by humans, that start to have real feelings and eventually achieve self-awareness. Imagine the legal quagmire this would create.  In this age of fast-moving and emerging technologies, the law sometimes struggles to keep pace with new scenarios, new crimes, new global platforms. What would happen if such robots, so much more efficient at doing many thousands of jobs than humans, became reality?  Facebook was fined £500,000 in 2018 for contravening Data Protection Laws in the Cambridge Analytica scandal – this is the amount they turn over in a little over five minutes, but it was the maximum fine under the Data Protection Act (1998). Under the new Data Protection Act (2018) which includes GDPR, the fine could have been up to £1.2 billion.  Main  Current Legislation  Introduce the topic of legislation relevant to IT systems. Ask students to name three laws. Students may struggle with this, so you could ask them to think in pairs, or to see if they can come up with three laws between the class.  A list of the laws to be covered is given on the next slide. Ask students if they can describe any of the main features of any of these laws. This will be useful to gauge their knowledge of the topic before you start the main teaching.  The laws listed are all given in the specification – so students need to know them all. Be aware that the specification gives the Data Protection Act (1998). This has been superseded by the Data Protection Act (2018) / GDPR.  Computer Misuse Act 1990  This is covered on the next few slides.  The punishments under the act are:   * Unauthorised access – up to 12 months imprisonment and/or fine (used to be 6 months before updated by the Police and Justice Act 2006) * Unauthorised access with intent to commit further offences – up to 5 years imprisonment and/or fine * Unauthorised modification of computer material – up to 10 years imprisonment and/or fine   Police and Justice Act 2006  This act amends and builds upon the Computer Misuse Act. The two main changes that affect computers are given on the slide. The act also increased the maximum sentence for unauthorised access to a computer system from six months imprisonment to two years.  Prior to 2006 it was legal to make, own and distribute hacking tools, examples of which are given on the following slide. This new law was controversial when first proposed as many people in cyber security need to use the same tools. As a result, making, owning or distributing hacking tools is only illegal if they are intended, or the person believes they might be used for computer misuse.  As such, students should be urged to err on the side of caution with respect to these tools. If they have a genuine educational or security reason to use them, it would make sense to first discuss this with a knowledgeable professional to see that they don’t breach this act.  **Denial of Service (DOS)** attacks (covered in Learning Aim D) are also addressed by the act.  There is a lot of information on websites about **Denial of Service (DOS)** attacks. Banks and financial institutions are common targets, but any site may be hit.  Titanium Stresser is described on the following web page:  <https://www.polygon.com/2017/4/26/15436320/teen-gets-2-year-prison-sentence-for-ddos-attacks>  <https://securelist.com/ddos-report-in-q1-2018/85373/> describes one in California:  “DDoS is also becoming more popular as a means of personal revenge. California, for instance, witnessed the case of David Goodyear, who was found guilty of trying to launch a DDoS attack against an amateur astronomy forum when it blacklisted him for using bad language.”  These attacks are expensive for organisations to deal with, and their reputations may be damaged when people cannot access their site.  DDOS attacks have become increasingly common, sometimes perpetrated with the aid of ‘bots’, fake email, social media or other accounts controlled by a single user.  An example of an attack is given on the next slide.  Give out **Worksheet 3** and ask students to do **Task 1**.  Topic 3 Worksheet 3  Topic 3 Worksheet 3 Answers  Consumer Rights Act 2015  This is a general law covering any item bought, including a digital product like software. The key part of the act is that products sold must be fit for purpose. If a charging cable broke after 10 years of heavy use this would clearly be fit for purpose, especially as most phones are replaced after two years. If though, it broke after 10 weeks of light use, it would not have been fit for purpose and the purchaser would be entitled to a repair or replacement.  Data Protection Act (1998, 2018) & GDPR  The first act to deal with data protection was in 1998. This act failed to keep up with the pace of change regarding personal data and computers of the next two decades. As such, a European regulation – the GDPR (General Data Protection Regulation) was created and came into effect in 2018. The UK implemented the Data Protection Act (2018) which incorporates the GDPR.  Data Protection Act (GDPR)  A good reference site on the need for data protection is  <https://www.itproportal.com/features/gdpr-and-the-ethical-use-of-data/>  Data Protection Act 2018  This Act incorporates the GDPR.  The six clauses of the Act are listed on the slide. The **rights of the user** are given on the following slide. Have any of the students ever taken advantage of these rights? They should be aware of them. Under the GDPR these requests are free.  Ask students to do **Task 2**. Students are asked to do some research on the Computer Misuse Act and the Data Protection Act.  Discuss their findings.  Employer’s duty of care  There are moral and ethical requirements for an employer as well as legal ones. See for example  <http://www.acas.org.uk/index.aspx?articleid=3751>  The legislation is designed to ensure that employers comply with their moral obligations. The image on the next slide shows children mending broken threads in a Georgia cotton mill. Without legislation pushed through by enlightened philanthropists, progress would be very slow, as is still seen in some developing countries.  Health and safety  Several slides describe the Health and Safety (Display Screen Equipment) Regulations 1992 and what they mean in practice.  Ask students whether their computer setup is conducive to correct body alignment (and whether they adopt correct body alignment.)  **Copyright**  Begin by discussing the ethics of copying work that someone else has created. Discuss the difference between plagiarism and copyright and the ethics of copying work and not acknowledging it.  Open source software is briefly mentioned at this point. It is covered in more detail in section A.  The Copyright, Designs and Patent Act 1988 and The Copyright (Computer Programs) Regulations 1992 are described on the next few slides  Ask students to do Tasks 3 and 4 on the worksheet.  The following sites are referred to in Task 3.  <https://www.comfort.txed.net/apps/pages/index.jsp?uREC_ID=336105&type=d&pREC_ID=743676>  <https://www.symantec.com/en/uk/about/legal/anti-piracy/types-piracy>  It may also be of interest that there are different types of software piracy as discussed on this webpage:  <https://www.symantec.com/en/uk/about/legal/anti-piracy/types-piracy>  Discuss answers to the worksheet tasks.  Plenary  Ask students to give two key features for each of the acts. This can be used to assess their improvement from the starter and also if there are any gaps that need to be covered again.  Give out **Homework 3**.  Topic 3 Homework 3  Topic 3 Homework 3 Answers |