Commons laws and regulations that must be followed when working with customers data:

The Data Protection Act (DPA) is a law that regulates the processing of personal data, ensuring that individuals' information is handled fairly, lawfully, and securely. It protects people and lays down rules about how data about people can be used by organisations, businesses or the government.

Importance of Data Protection Act:

1. Protects individuals' rights and freedoms, particularly their right to privacy.
2. Promotes transparency and accountability in data handling practices.
3. Helps prevent data breaches and cyber-attacks.
4. Ensures that organisations handle personal data in a responsible and secure manner.

Real-world example how to follow Data Protection Act:

Suppose you're a marketing manager at a company, and you're collecting email addresses from customers to send newsletters. To follow the DPA, you would:

1. Clearly inform customers that you're collecting their email addresses and explain how you'll use them.
2. Obtain explicit consent from customers before sending them newsletters.
3. Provide an easy way for customers to opt-out of receiving newsletters.
4. Store the email addresses securely and only share them with authorized personnel.

Impact on working with data:

The DPA has a significant impact on working with data, as it requires organisations to:

1. Implement robust data protection policies and procedures.
2. Conduct regular data audits and risk assessments.
3. Train employees on data protection best practices.
4. Use secure technologies and encryption methods to protect personal data.
5. Respond promptly to data breaches and notify affected individuals.

Consequences of breaching the DPA:

If an organisation breaches the DPA, it can face:

1. Significant fines: Up to £17 million or 4% of the organisation's global annual turnover.
2. Reputation damage: Loss of customer trust and damage to the organisation's reputation.

3. Legal action: Individuals can take legal action against the organisation for damages.
4. Regulatory action: The relevant data protection authority can take enforcement action, including audits and inspections.

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in and outside of the European Union (EU). Although the UK has left the EU, the GDPR has been incorporated into UK law as the UK GDPR.

Importance of GDPR:

1. Protects individuals' personal data and rights.
2. Promotes transparency and accountability in data handling practices.
3. Helps prevent data breaches and cyber-attacks.
4. Ensures that organisations handle personal data in a responsible and secure manner.

Real-world example how to follow GDPR:

Suppose you're a UK-based charity that collects donations and stores donor information. To follow UK GDPR, you would:

1. Clearly inform donors about the personal data you collect (e.g., names, addresses, phone numbers) and explain how you'll use it.
2. Obtain explicit consent from donors before collecting and processing their personal data.
3. Provide donors with easy access to their personal data and allow them to correct or delete it.
4. Implement robust security measures to protect donor data, such as encryption and secure payment processing.

Impact on working with data:

UK GDPR has a significant impact on working with data, as it requires organisations to:

1. Conduct data protection impact assessments to identify and mitigate data protection risks.
2. Implement data protection by design and by default, ensuring that data protection is integrated into all processes and systems.
3. Appoint a Data Protection Officer (DPO) to oversee data protection compliance.
4. Establish clear data retention and deletion policies.
5. Use secure technologies and encryption methods to protect personal data.

Consequences of breaching UK GDPR:

If an organisation breaches UK GDPR, it can face:

1. Significant fines: Up to £17 million or 4% of the organisation's global annual turnover.
2. Reputation damage: Loss of customer trust and damage to the organisation's reputation.
3. Legal action: Individuals can take legal action against the organisation for damages.
4. Regulatory action: The Information Commissioner's Office (ICO) can take enforcement action, including audits and inspections.
5. Suspension or ban on data processing: In severe cases, the ICO can suspend or ban data processing activities.

The Freedom of Information Act (FOIA) is a law that allows individuals to access information held by public authorities, such as government departments, local councils, and other public bodies. The FOIA aims to promote transparency, accountability, and openness in government.

Importance of Freedom of Information Act:

1. Promotes transparency: **FOIA** allows citizens to access information, enabling them to hold public authorities accountable for their actions.
2. Encourages accountability: By providing access to information, **FOIA** helps to prevent corruption, mismanagement, and abuse of power.
3. Supports informed decision-making: **FOIA** enables citizens to make informed decisions by providing access to relevant information.

Real-world example how to follow FOIA:

Suppose you're a journalist investigating a local council's decision to develop a new housing project. To follow the FOIA, you would:

1. Submit a written request to the council, specifying the information you're seeking.
2. Clearly state your name and contact details.
3. Be prepared to pay a fee (if applicable) for the council to process your request.
4. Receive a response from the council within 20 working days, either providing the requested information or explaining why it cannot be disclosed.

Impact on working with data:

1. Data disclosure: Public authorities must disclose information upon request, unless exemptions apply.
2. Data management: Public authorities must maintain accurate and up-to-date records to facilitate information disclosure.
3. Transparency: **FOIA** promotes a culture of transparency, encouraging public authorities to be more open and accountable.

Consequences of breaching the FOIA:

1. Financial penalties: Public authorities may face fines or penalties for failing to comply with **FOIA** requests.
2. Reputation damage: Non-compliance can damage the reputation of public authorities and erode trust.
3. Investigations and enforcement: The Information Commissioner's Office (ICO) can investigate and enforce compliance with the **FOIA**.
4. Court action: Individuals can take court action against public authorities for failing to comply with **FOIA** requests.

The Computer Misuse Act (CMA) is a law in the United Kingdom that makes it a criminal offense to access or modify computer systems or data without authorisation. The **CMA** aims to prevent and punish unauthorized access, use, or interference with computer systems, networks, and data.

Importance of Computer Misuse Act (CMA):

1. Protects computer systems and data: The **CMA** helps prevent unauthorized access, theft, or damage to computer systems and data.
2. Deters cybercrime: By making unauthorized access a criminal offense, the **CMA** deters individuals and organisations from engaging in cybercrime.
3. Promotes cybersecurity: The **CMA** encourages organisations to implement robust security measures to protect their computer systems and data.

Real-world example how to follow CMA:

Suppose you're an IT administrator at a company, and you need to access a colleague's computer to troubleshoot an issue. To follow the **CMA**, you would:

1. Obtain explicit permission from your colleague or supervisor before accessing the computer.
2. Ensure you have the necessary authorisation and credentials to access the computer.
3. Only access the computer for the specific purpose of troubleshooting and avoid accessing any unauthorized data.

4. Document the access and any actions taken, including the reason for access and the outcome.

Impact on working with data:

1. Authorisation and access controls: Organisations must implement robust access controls and ensure that only authorized personnel can access computer systems and data.
2. Data protection: The **CMA** emphasizes the importance of protecting data from unauthorized access, theft, or damage.
3. Incident response: Organisations must have incident response plans in place to respond to unauthorized access or other security incidents.

Consequences of breaching the CMA:

1. Criminal prosecution: Individuals who breach the **CMA** can face criminal prosecution, fines, and imprisonment.
2. Civil liability: Organisations can face civil liability for damages resulting from unauthorized access or other security incidents.
3. Reputation damage: Breaches of the **CMA** can damage an organisation's reputation and erode trust with customers and partners.
4. Regulatory action: Regulators can take enforcement action against organisations that breach the **CMA**, including fines and penalties.

Describe, with examples, the **three** major areas that the Computer Misuse Act deals with.

The **Computer Misuse Act 1990** is a UK law designed to address various types of computer-related crime. It covers three major areas, each of which is aimed at protecting individuals, organisations, and public infrastructure from malicious activities. Here's a breakdown of the three major areas, along with examples:

Area	Description	Example
Unauthorised Access to Computer Material	This area deals with hacking or accessing a computer system or data without permission. It includes unauthorised access to files, networks, or systems.	A person hacks into a company's server to access sensitive information like personal data or trade secrets without authorisation.
Unauthorised Access with Intent to Commit or Facilitate the Commission of Further Offences	This involves gaining unauthorised access to computer systems or data with the intention of committing other criminal acts, such as fraud or theft.	A hacker breaks into an online banking system to steal money from users' accounts or to install malware for later access.
Unauthorised Modification of Computer Material	This area criminalises the act of altering, deleting, or modifying computer data or programs without authorisation, potentially causing damage or harm.	A cybercriminal deletes important files from a government database or installs malicious software that corrupts a company's network.

These areas are aimed at preventing a wide range of cybercrimes, from hacking to data manipulation, ensuring the security of computer systems and the information they store.

The computer misuse act 1990 is an act where an individual can be criminalised because of computer related offense. Describe three extra powers that the Police and Justice Act 2006 (Computer Misuse) has added.

Description
Unlawful Possession of Articles for Use in Computer Misuse Offenses: The Act introduced an offense for the possession of articles (such as hacking tools or malware) with the intent to use them for committing computer misuse offenses. This provision enables law enforcement to take action against individuals even before an actual crime is committed, targeting the tools that could facilitate computer crimes.
Amendment to Sentences for Computer Misuse Offenses: The Act increased the severity of penalties for certain computer-related offenses. For example, it introduced harsher sentencing for those convicted of committing unauthorised access or damage with the intent to cause serious harm. This includes a potential life sentence in the most severe cases.
Offense of Unauthorised Access with Intent to Commit or Facilitate Further Offenses: A new offense was created under the Act that targets individuals who access computer systems without authorisation, intending to commit or facilitate another criminal act (such as fraud or terrorism). This power extends the scope of the Computer Misuse Act, making it easier to prosecute individuals whose actions might aid or prepare other criminal activities.

Three items of data which a company can store about an employee.
Personal Identification Information: This includes details like the employee's full name, date of birth, address, and contact information (phone number and email). This data is essential for HR purposes, communication, and legal compliance.
Employment History and Job Details: This covers information such as job title, department, work history within the company, salary, performance reviews, and dates of employment. It helps track an employee's role and progression within the company.
Payroll and Tax Information: This includes salary, bonuses, tax information (e.g., National Insurance number in the UK, tax withholding details), and banking information for salary deposits. It is used for compensation, benefits, and tax purposes.

Three more examples of data that an employer can only store if they first get the employee's permission.
Health and Medical Information: Any data related to the employee's physical or mental health, such as medical conditions, disability status, or sick leave records, typically requires explicit consent from the employee. This information is often sensitive and governed by strict data protection regulations.
Biometric Data: If an employer collects biometric information (e.g., fingerprints, facial recognition data, or retina scans) for security or attendance purposes, the employee's permission is necessary. This type of data is considered particularly sensitive.
Personal or Sensitive Social Media Information: If an employer seeks to access or store personal social media profiles or activities (for example, to monitor an employee's online presence), explicit consent must be given by the employee. This can also extend to any personal data gathered through public online activity that is unrelated to the job.

Further research to answer the below questions.

Question	Answer
Example of: Copyright infringement	A person downloads and distributes a **pirated version of a movie** without permission from the copyright holder. This act violates the copyright laws of the original creators, as they have exclusive rights to distribute, reproduce, and sell copies of their work. By sharing the unauthorised copy, the individual is infringing upon the copyright owner's rights.
Example of: Plagiarism	A student submits a research paper for a class, copying large sections of text directly from an online article without giving proper credit to the original author. The student presents the work as their own, failing to cite the source of the copied material. This is plagiarism because the student is using someone else's ideas or words without acknowledgment, violating academic integrity rules.

Two consequences of copyright infringement and software piracy	**Legal Penalties**: Individuals or businesses found guilty of copyright infringement or software piracy may face significant legal consequences, including **fines** and **lawsuits**. In some cases, copyright holders can seek damages through civil lawsuits, and criminal cases could result in **imprisonment**. For example, software piracy could lead to hefty fines and jail time, depending on the scale of the infringement. **Financial Losses and Damaged Reputation**: Copyright infringement and software piracy can result in **financial losses** for creators or companies due to lost sales or royalties. Additionally, businesses or individuals caught engaging in piracy may suffer from a **damaged reputation**, which can undermine consumer trust, harm brand image, and lead to loss of future opportunities or partnerships. This can be especially damaging in industries reliant on intellectual property, like media, technology, and entertainment.
Three possible consequences for individuals when using pirated software	**Legal Consequences**: Using pirated software is illegal and can result in **fines** or even **criminal charges**. Individuals caught using or distributing pirated software can be held liable for copyright infringement, potentially facing costly legal action. **Security Risks**: Pirated software often comes with **malware** or **viruses** that can compromise the security of a user's device. These malicious programs may steal personal data, corrupt files, or damage the system, leading to potential data breaches or identity theft. **Lack of Support and Updates**: Pirated software does not receive official **updates** or **technical support** from the software developer. This means that the software may become outdated, vulnerable to security issues, and lack essential features or fixes, ultimately affecting its performance and functionality.