Safety and Security

Physical Safety

Health Aspects

- *Health and safety regulations advise that all computer systems have at least tiltable and anti-glare screens, adjustable chairs and foot supports, suitable lighting and uncluttered work stations, and recommend frequent breaks and frequent eye tests.*

Safety Aspects

Safety Risk	Ways of eliminating or minimising risk
Electrocution	• Use an RCB (residual current breaker) • Check insulation on wires regularly • Don't allow drinks near computers • Check equipment on a regular basis
Trailing wires (trip hazard)	• Use cable ducts to make the wires safe • Cover wires and/or have them tucked away • Use wireless connections wherever possible, thus eliminating cables
Heavy equipment falling and causing injury	• Use strong desks and tables to support heavy hardware • Use large desks so that hardware isn't too close to the edge where it can fall off
Fire risk	• Have a carbon dioxide/dry fire extinguisher nearby • Don't cover equipment vents • Make sure that the electrics used in the hardware are fully maintained • Ensure good ventilation • Don't overload sockets with too many items • Change to low voltage hardware wherever possible

Minimising safety risks

- Check the stare of wires/cables/plugs regularly
- Make sure that drinks are kept away from the computer
- Fix wires along walls/desk to avoid direct contact with people
- Don't cover computers with paper/fabric- prevent ventilation
- Don't plug too many devices into an electric outlet socket-overloading a socket can cause a fire
- Take regular exercise every hour
- Carry out an ergonomic assessment on your work station

E-Safety

- Personal data refers to any data concerning a living person who can be either identified from the data itself or from the data in conjunction with other information (e.g. name, address, DOB, medical history, banking details etc.)

- If personal data is leaked, it may lead to: identity theft, bank fraud, damages to personal property, kidnapping
- To prevent the above it is essential that personal data is protected
- If a student shares a photograph of themselves in their school uniform on social media, then paedophiles, kidnappers etc. can physically reach the student

Internet safety

- To keep personal data safe, one must:
  i. Not give unknown people personal data or send pictures of themselves to them
  ii. Maintain privacy settings to control which cookies are on their computer
  iii. Use learner friendly search engines and websites recommended by educational institutions
  iv. The website being accessed is from a trusted source or has a padlock symbol/ https protocol (s for secure)

Email Safety

- Open emails only from known sources, and do not click on emails with hyperlinks without confirming the sender of the email. Think before opening an email from an unknown person, never send any other sensitive information
- Ask their ISP to enable email filtering to classify spam mails as spam

Social Media Safety

- Block and report users who seem suspicious or use inappropriate language
- Never use a real name, only use a nickname
- Use appropriate language
- Do not enter chat rooms, as users can lure you into giving personal information by seeming too nice
- Do not meet anyone off the internet for the first time on your own, or at least speak to a trusted adult first
- Do not misuse images
- Respect the confidentiality of other uses

Online Games

- Similar measures apply to that taken when using social media
- Additionally, players should be careful about:
  i. In-game violence
  ii. Cyber bullying
  iii. Keeping their webcams off
  iv. Predators may use voice masking technology to lure a user to reveal their age, sex etc.
  v. Cyber-attacks involving viruses, ransomware etc.

Security of Data

Effective security of data

Hacking

This is the act of gaining unauthorised access to a computer system

- This can lead to identity theft or the misuse of personal information
- Data can be deleted, changed or corrupted on a user's computer
- Use of encryption won't stop hacking-it makes the data unreadable to the hacker but the data can still be deleted, altered or corrupted
- Can be minimised by:
  - i. Use of firewalls
  - ii. Use of strong (frequently changed) passwords and user IDs
  - iii. Use of intrusion detection software
  - iv. Use of user IDs and passwords

User IDs

- To log on to a network, a user must type in a user ID
- User ID assigns user privilege once user logs in
- The top level privilege for a network is an administrator:
  Able to set passwords and delete files from server etc.
- User privilege may only allow to access their own work area

Passwords

- After typing in user ID, the user will be requested to type in their password
- Generally, it is a combination of letters and numbers
- Passwords are shown as stars (***) so nobody overlooking can see it
- Many systems ask for password to be typed in twice as a verification check, in case of input errors
- If password is forgotten, administrator must reset it
- If password is forgotten on a website, it will be sent to your e-mail

Biometric Data

- Uses features if the human body unique to every individual, such as fingerprints, retina, iris, face and voice recognitions. It is used in authentication techniques as it is very difficult/impossible to replicate

Advantages	Disadvantages
• Usernames and passwords don't have to be remembered • Almost impossible to replicate body parts • Somebody else can't gain access, like with a stolen card • They can't be forgotten, like a card	• The readers are expensive • Damages in fingerprints can deny access • Some people worry about their personal information being stored

Security of data online

Digital Certificate

- A digital certificate is an electronic passport used in the security of data sent over the internet
- They can be attached with mails so that the receiver can know that the mail is from a trusted source

Secure Socket Layer (SSL)

- Type of protocol that allows data to be sent and received securely over the internet
- When a user logs onto a website, SSL encrypts the data
- https or padlock in the status bar
- When a user wants to access a secure website:
  i. User's web browser sends a message, so it can connect with required website which is secured by SSL
  ii. Web browser requests that the web server identifies itself
  iii. Web server responds by sending a copy its SSL certificate
  iv. Web browser checks if certificate is authentic
  v. Sends signal back to web browser
  vi. Starts to transmit data once connection is established
  vii. If not secure, browser will display an open padlock

Features of a secure webpage

- The webpage URL is secure, it will start with 'https' instead of 'http'
- Padlock sign

Phishing

The creator sends out legitimate looking emails to target users. As soon as the recipient clicks on a link in the email or attachment, they are sent to a fake website or they are fooled into giving personal data in replying to the email. The email often appears to come from a legitimate source.

- The creator of the email can gain personal data, such as bank account data or credit card numbers, from the user
- This can lead to fraud or identity theft
- How damage by phishing is minimised:
  i. Many ISPs or web browsers filter out phishing emails
  ii. Users should always be cautious when opening emails or attachments
  iii. Don't click on attachments that end in –exe., .bat, .com or .php., for example