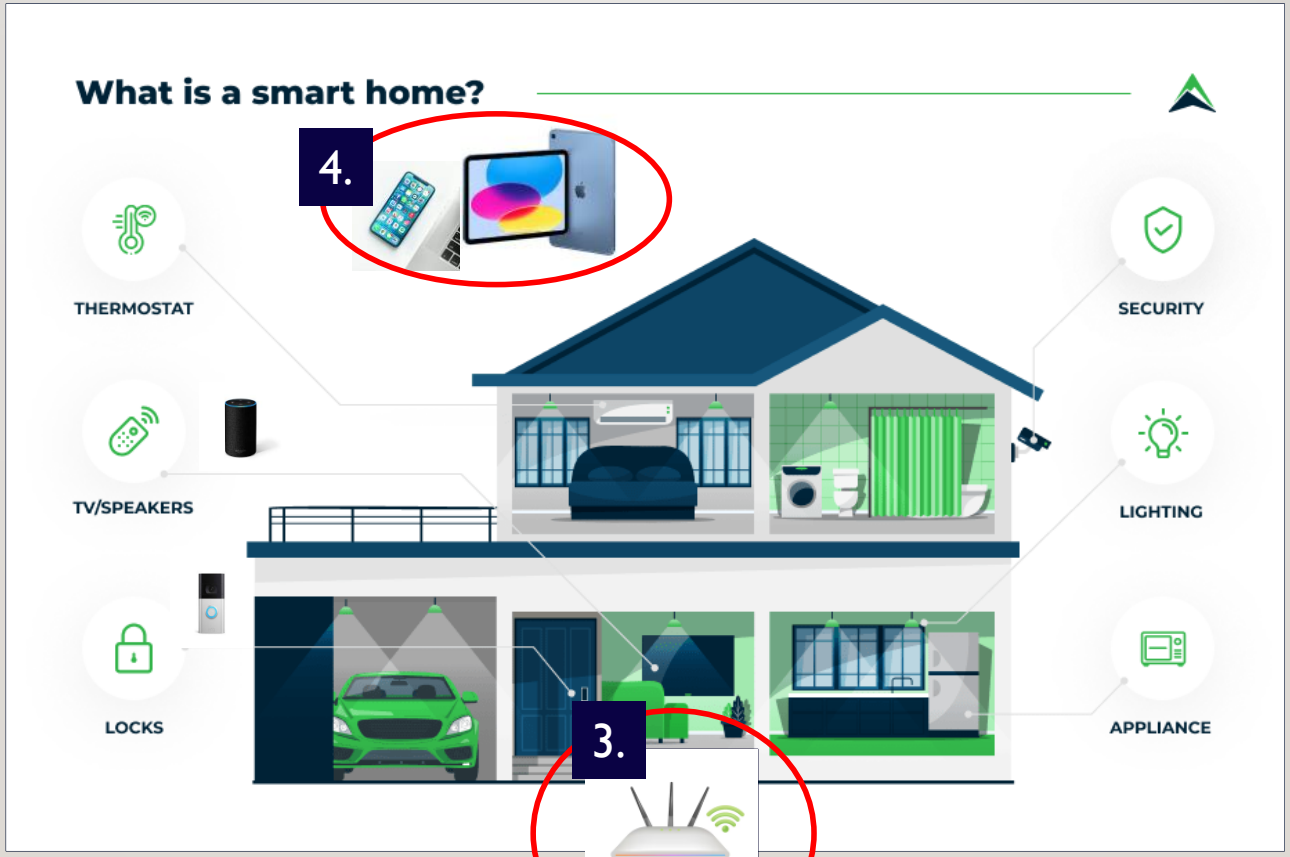
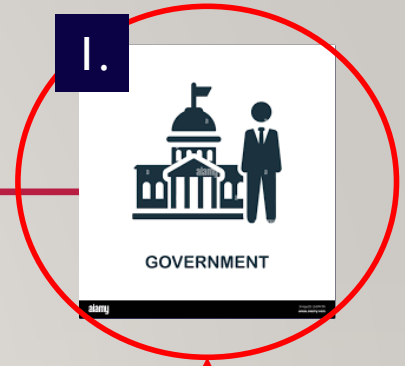
# TECHNOLOGY IN THE HOME

Layers of Security and Technologies Available

# LAYERS OF SECURITY

1. Governments
   Legislation
2. Internet Providers
   Filtering/Encryption
3. Home Router
   Parental Controls
4. Devices
   Passwords
   Parental Controls




# 1. GOVERNMENTS

Department for Science, Innovation & Technology

**UK Online Safety Act**

- Set of laws that protects children and adults online.
- It puts a range of new duties on social media companies and search services, making them more responsible for their users' safety on their platforms.
- Platforms will be required to prevent children from accessing harmful and age-inappropriate content and provide parents and children with clear and accessible ways to report problems online when they do arise.

**Ofcom**

- Independent regulator of Online Safety. It will set out steps providers can take to fulfil their safety duties in codes of practice. It has a broad range of powers to assess and enforce providers' compliance with the framework.

# UK ONLINE SAFETY ACT – CRIMINAL OFFENCES

**The criminal offences introduced by the Act comes into effect in April. These offences cover:**

- Encouraging or assisting serious self-harm
- Cyberflashing
- Sending false information intended to cause non-trivial harm
- Threatening communications
- Intimate image abuse
- Epilepsy trolling

These new offences apply directly to the individuals sending them, and convictions have already been made under the cyberflashing and threatening communications offences.

Department for Science, Innovation & Technology

Department for Science, Innovation & Technology

# UK ONLINE SAFETY ACT - CONTENT THAT IS HARMFUL TO CHILDREN

Companies with websites that are likely to be accessed by children need to take steps to protect children from harmful content and behaviour.

The categories of harmful content that platforms need to protect children from encountering are set out in the Act. Children must be prevented from accessing Primary Priority Content and should be given age-appropriate access to Priority Content.

**Primary Priority Content**

- Pornography
- Content that encourages, promotes, or provides instructions for either:
  - Self-harm
  - Eating disorders
  - Suicide

**Priority Content**

- Bullying
- Abusive or hateful content
- Content which depicts or encourages serious violence or injury
- Content which encourages dangerous stunts and challenges; and
- Content which encourages the ingestion, inhalation or exposure to harmful substances.

# UK ONLINE SAFETY ACT - HOW THE ACT PROTECTS WOMEN AND GIRLS

Department for Science, Innovation & Technology

The most harmful illegal online content disproportionately affects women and girls, and the Act requires platforms to proactively tackle this. Illegal content includes harassment, stalking, controlling or coercive behaviour, extreme pornography, and revenge pornography.

All user-to-user and search services have duties to put in place systems and processes to remove this content when it is flagged to them. The measures companies must take to remove illegal content will be set out in Ofcom's codes of practice.

# 2. INTERNET SERVICE PROVIDERS (ISP)

Providers currently protect their customers by monitoring web traffic to determine how and when the network is being used. The below are some of the strategies employed to help keep customers safe.


**Intrusion Detection System**

Think of an intrusion detection system (IDS) as a digital alarm system. ISPs use them to detect suspicious activity on their networks and alert security personnel.


**Firewall Implementation**

ISPs install robust firewalls to block potentially harmful traffic. Like a gatekeeper, the firewall checks each data packet to ensure it's safe before allowing it through.

**Threat Monitoring**

ISPs are like digital watchtowers, monitoring traffic for signs of malicious activity. They can identify patterns that might indicate a cyber threat, like a sudden surge in traffic or unusual data patterns.

# 3. INTERNET CONNECTION SECURITY

- Broadband Routers - The standard home internet routers provide by local internet companies (JT Global, Sure etc.) are more basic in nature and provide little filtering or security options. It is recommended to replace these with one that provides more security in general. The below have been selected based on their ability to provide additional parental security.

| Router Model | Cost |
|---|---|
| TP-Link Archer C80 | $ |
| TP-Link AC1200 | $$$ |
| ASUS RT-AX57 | $$ |
| Synology RT2600ac | $$$ |
| Asus ROG Rapture GT-AX11000 | $$$$$ |

# 4. COMPUTER & LAPTOP SECURITY

- Antivirus – Important to ensure laptops or desktop computers are protected. Many security companies provide free versions of their antivirus software. This will provide basic protection, with paid-for versions providing a greater amount of security.

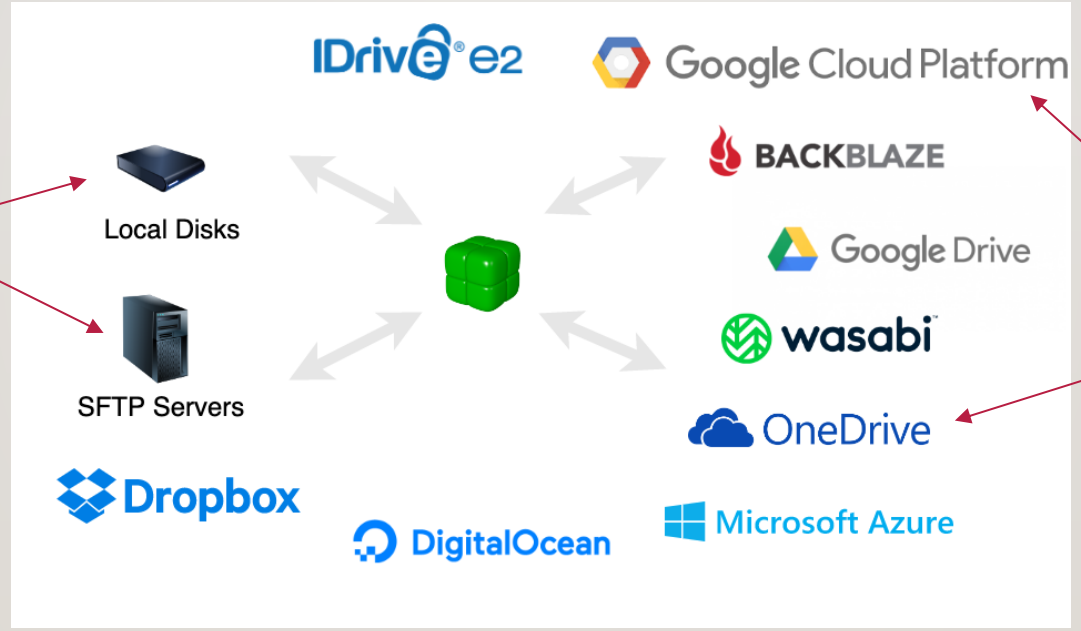
- Well established companies;
  - McAfee
  - Norton
  - AVG


# DATA BACKUPS – CLOUD VS PHYSICAL

- A physical backup stores data on a local device like a hard drive or tape, while a cloud backup stores data on remote servers accessible through the internet, meaning physical backups are physically present on your computer while cloud backups are stored off-site on a third-party server, providing greater accessibility and protection against local disasters like fires or floods
- Cloud backup is a service that stores copies of your files, applications, and other data on remote servers. You can access these copies through the internet.

# DATA BACKUPS

Physical Backups




Cloud Backups

# TABLET COMPUTERS

1

Create child-only accounts. This will restrict the access and applications available.

2

Define a “usage policy” with children;

- How long they can spend on a tablet
- Where they can use it – i.e., front room only

3

Use parental controls and age-restricted apps

# SMART TV'S

Nowadays, most TVs are smart and allow us to access streaming platforms like Netflix, Disney+, Prime Video and BBC iPlayer. But being 'smart' goes beyond that. Some of these TVs support voice control, which means you can do pretty much everything you would with a regular remote, just by talking.


- Consider location of Smart TV's – Are bedrooms a good idea?
- Connect the Smart TV to a secure internet connection
- Discuss what the children would like to watch.
- On Demand services
  - Many services (Netflix, Disney) have children accounts
  - PIN protect adult accounts to ensure children don't access those profiles

# SMART SPEAKERS

Become familiar with your smart speaker privacy and security settings. Dive into your device's app to explore your options. Google, Amazon, and Apple have been rolling out their own settings to lower safety risks for users.

Mute the microphone when you don't want to be heard. Some devices have a physical switch, while others can be deactivated by voice command. This can prevent misfired wake phrases.

Delete your command history to erase local and cloud storage of past recordings. This information is used to understand your voice better, however not regularly deleting this could risk your security. Commands can be deleted on most services either individually, in a time range, or in full.

Opt-out of data sharing for "improving" voice services or "personalizing" your experience. Many times, these options are on by default. You'll have to turn these off yourself to halt the activity.

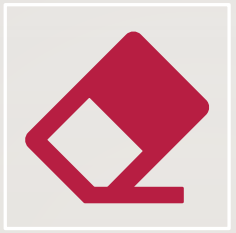
Consider having different networks for your IoT devices and make sure these are separate from the home Wi-Fi you use for your personal devices (i.e., non IoT devices).

# BUYING OR SELLING USED DEVICES

## Before you wipe a device

Ensure any data is backed up

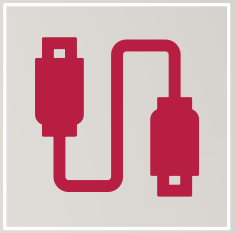
If you use your device to verify other accounts (for example, by entering codes sent by text message), make sure you can do this on another device before you erase any data.



## Erasing the data on your device

To erase all data, use your device's Erase all Content and Settings or Factory reset feature

You may be given the option to keep your personal files. Do not choose this option if you're not keeping your device.



## Choosing a secondhand device

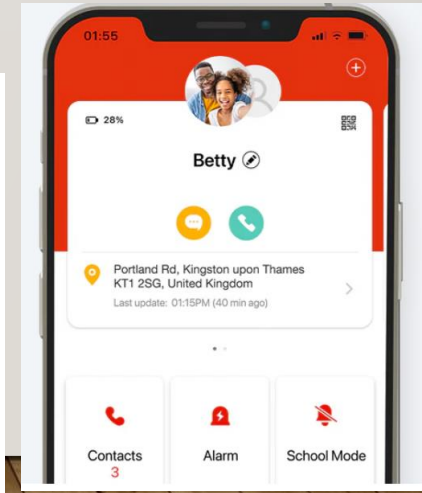
If a device isn't supported it won't receive security updates from the manufacturer, and without those the device is easier to hack.

Check online to see if the model you're considering can still receive updates from the manufacturer.

# ALTERNATIVES TO SMARTPHONES

- Brick Phones - A "brick phone" is considered a safer option for children than a smartphone because it typically only allows for basic calling and texting functions, preventing access to the internet and social media which can expose children to potentially harmful content and cyberbullying, thus promoting greater child safety; essentially, it limits their digital exposure to only necessary communication features.


- Xplora Watches - Xplora smartwatches are designed to keep children safer. They allow you to stay connected throughout the day like a cell phone. However, they have no access to the internet, social media, and pre-approved contacts, Xplora smartwatches are a perfect alternative.

# ANY QUESTIONS?