

# RSA<sup>®</sup>Conference2019

San Francisco | March 4–8 | Moscone Center



**BETTER.**

SESSION ID: MBS-F03

## Changing the World with the UK's Code of Practice for Consumer IoT Security

**David Rogers**

Mobile Technology, Cyber Security &  
Standards Adviser  
Department for Digital, Culture, Media &  
Sport (DCMS), UK  
@drogersuk



#RSAC

# IoT Insecurity





# Secure by Design

- UK National Cyber Security Strategy:

“the UK is more secure as a result of technology, products and services having cyber security designed into them by default”



# Review

- Primarily address two key risks related to consumer IoT:
  - Poorly secured IoT devices and associated services increasingly threaten consumers' online security, privacy and even safety.
  - Poorly secured devices are likely to be hijacked and can be used in large-scale DDOS attacks (e.g. mirai botnet). The impact is felt by third parties rather than the end user.



# UK Government Approach

- 2017 - 2018:
  - Cooperation with industry, academia, consumer associations and international partners
- March 2018:
  - Policy report
- October 2018:
  - Code of Practice for Consumer IoT Security
  - Mapping of the Code to existing recommendations
  - Consumer guidance
- <https://www.gov.uk/government/publications/secure-by-design>



Department for  
Digital, Culture,  
Media & Sport



Department for  
Digital, Culture  
Media & Sport

Secure by Design: Improving the cyber  
security of consumer Internet of Things  
Report



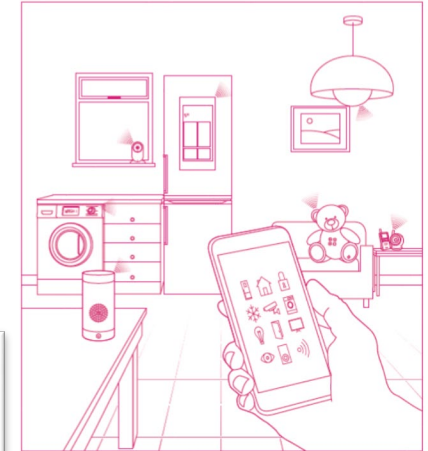
Department for  
Digital, Culture,  
Media & Sport

Mapping of IoT Security Recommendations,  
Guidance and Standards to the UK's Code of  
Practice for Consumer IoT Security

October 2018

Department for  
Digital, Culture,  
Media & Sport

## Code of Practice for Consumer IoT Security



October 2018

## Consumer Guidance for Smart Devices in the Home

Smart or internet-connected devices, such as smart TVs, music speakers, connected toys or smart kitchen appliances can bring great benefits to your daily life. However, without taking steps to secure all of your internet-connected products, you and your data could be at risk from someone getting unauthorised access to your device or account. Developed by the UK government and industry experts, this guidance will help you manage the security of your devices and help protect your privacy.



### SETTING-UP YOUR DEVICE

- Read and follow the set-up instructions for the device. These are often found in an app downloaded onto your smartphone, tablet or from a paper manual and guide that comes with the product.
- Check device instructions to see if you need to create an account on the manufacturer's website, or download any other recommended apps.
- If you are prompted to enter a password during the set-up process that is easy to guess, (such as 'admin' or '000000'), you should change it. Guidance on creating a strong password can be found on the Cyber Aware website.

### MANAGING YOUR ACCOUNT

- To set-up and manage your device, you may need to create or use an existing account on the manufacturer's website. This account may allow you to add a new device or link your smartphone to your devices. You should ensure that your account has a strong password.
- For added security, if the device or app offers Two Factor Authentication which provides a second layer of security, (such as a text message to your phone) you should enable it. This is particularly important if the account contains your personal data or sensitive information or is linked to something that may impact your or another person's physical safety.
- Some products allow you to access or control them when you are away from your home's Wi-Fi network; such as, to view security camera footage. Consider whether you need to make use of this feature, as products may allow you to disable it either in the app settings or within your account.

### KEEP UPDATING YOUR SOFTWARE AND APPS

- Much like your laptop and smartphone, software and app updates help keep your devices secure. You should:
  - Check whether you can set-up and enable automatic updates (on the app or on your online account).
  - Install the latest software and app updates. These updates should download and install automatically on your device. If not, then you should install them straight away so you have the latest security protections. You should be prompted when a new update is ready to install, usually via a pop-up message or in the settings menu in the app or device menu.

### IF YOU BECOME AWARE OF AN INCIDENT AND THINK IT AFFECTS YOUR DEVICE

- Visit the manufacturer's website to see if there is information available on what you should do next.
- Check the National Cyber Security Centre and the Information Commissioner's Office websites to see any published guidance.
- Further advice on your consumer rights can be found on the Which? and Citizens Advice websites.



UK Government

CYBER AWARE

www.cyberaware.gov.uk

**BBC** News Sport More Search

# NEWS

Home UK World Business Politics Tech Science Health More

Technology

## UK seeks to secure smart home gadgets

15 October 2018

Share

**Which?** News All news

Technology ▶ Smart homes

## How new guidelines on smart devices will help protect consumers from being hacked

*Tech companies HP Inc and Centrica Hive are the first to commit to making their products 'secure by design'*

**FINANCIAL TIMES**

Cyber Security: Internet of Things

Cyber Security Added

## Manufacturers face tighter rules on devices

'It's going to take collective action to get the security outcomes we're looking for'

**MailOnline** WIRES

Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science | Money | V

Wires Home

## Smart device-makers issued with code of practice to improve cyber security

By PRESS ASSOCIATION  
PUBLISHED: 13:19, 15 October 2018 | UPDATED: 13:19, 15 October 2018

Share

Unique passwords, timely software updates and secure storage of personal data are among Government guidelines set out in a new code of practice for smart home device makers.

**The Telegraph** ALL SECTIONS Technology Intelligence More

Technology Intelligence

## Tech giants to sign up to new code of conduct to reduce risk of cyber attacks

Save 1

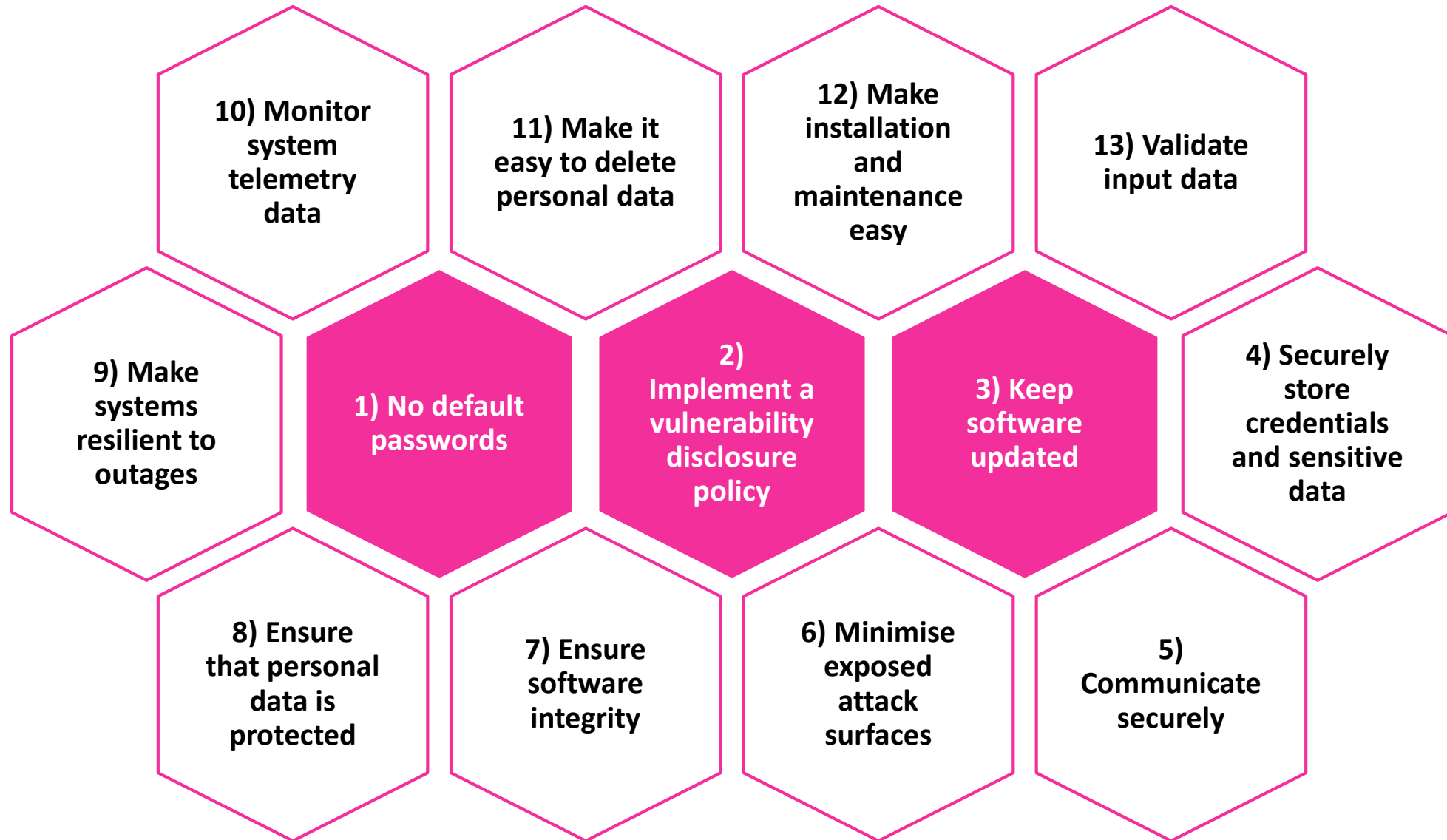
# UK Code of Practice for Consumer IoT Security

- 13 outcome-focused, high-level guidelines.
- Brings together what is widely considered good practice.
- Focuses on what matters most. Not a silver bullet to all problems.
- Primary audience: device manufacturers.





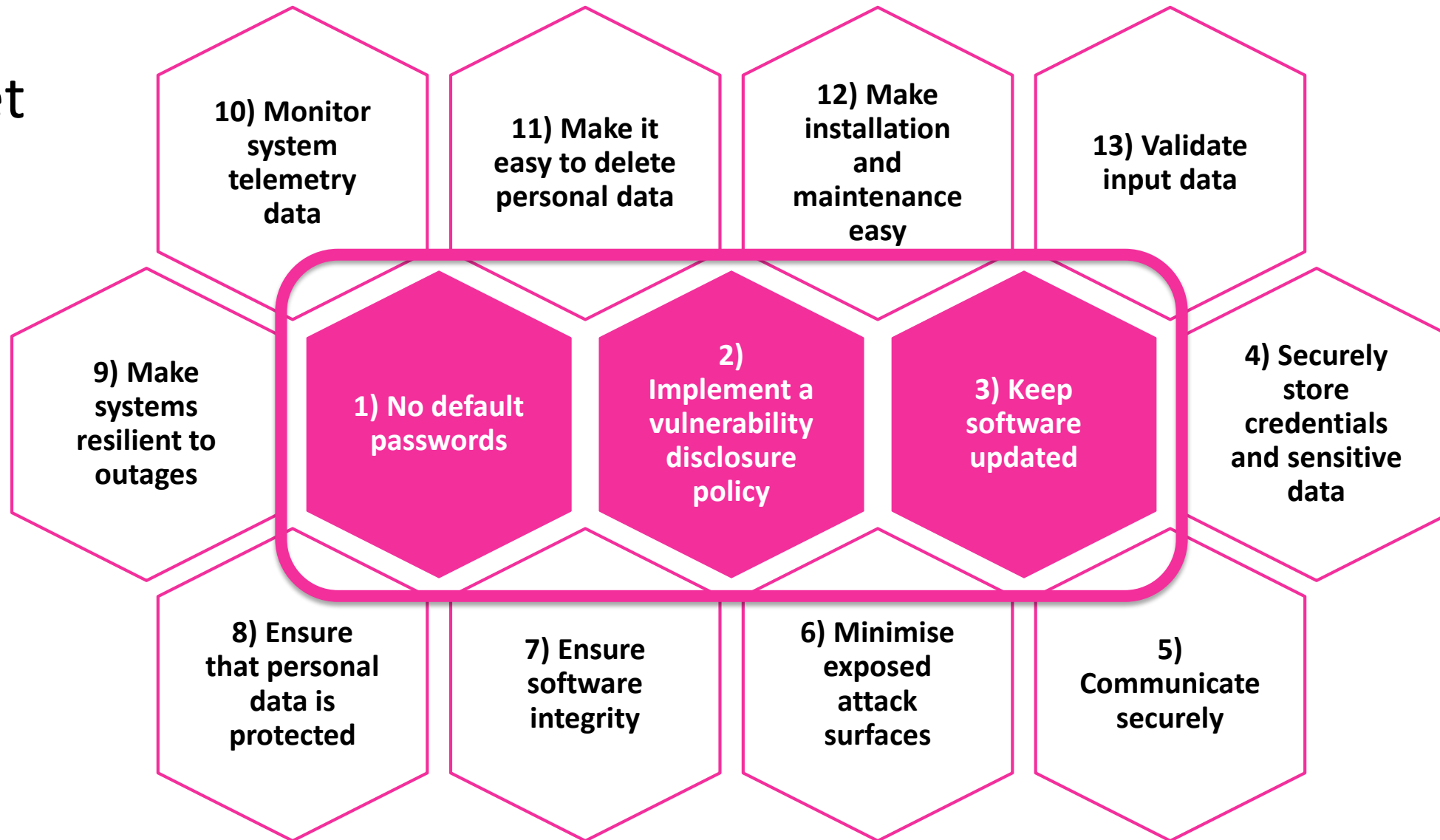
# UK Code of Practice for Consumer IoT Security





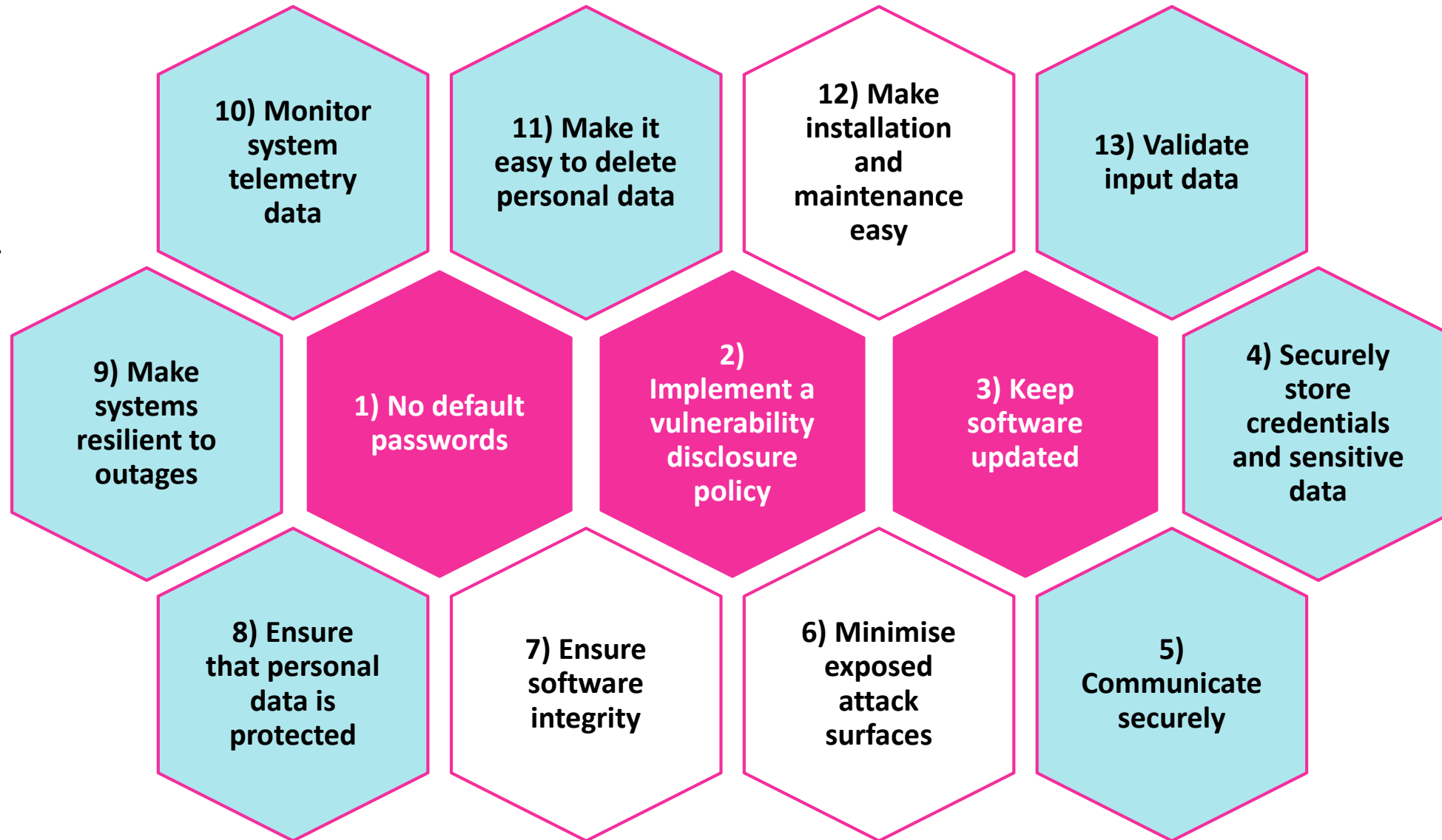
# UK Code of Practice for Consumer IoT Security

- Top 3 – Get the basics right!



# UK Code of Practice for Consumer IoT Security

- Seven are aligned with GDPR (2018)



- 
- Legend**
- Opposite
  - Publication
  - Government
  - Standards
  - Academic
  - Industry
  - Industry Association
  - Think tank
  - Not for profit



# Pledges to implement the Code of Practice

- IoT manufacturers that have made a public commitment to implement the Code of Practice:



# Development of an ETSI TS on Consumer IoT Security



ETSI TS 103 645



# Consumer Guidance

## Consumer Guidance for Smart Devices in the Home

Smart or internet-connected devices, such as smart TVs, music speakers, connected toys or smart kitchen appliances can bring great benefits to your daily life. However, without taking steps to secure all of your internet-connected products, you and your data could be at risk from someone getting unauthorised access to your device or account. Developed by the UK government and industry experts, this guidance will help you manage the security of your devices and help protect your privacy.



### SETTING-UP YOUR DEVICE

- **Read and follow the set-up instructions** for the device. These are often found in an app downloaded onto your smartphone, tablet or from a paper manual and guide that comes with the product.
- **Check device instructions to see if you need to** create an account on the manufacturer's website, or download any other recommended apps.
- If you are prompted to enter a password during the set-up process that is easy to guess, (such as 'admin' or '00000'), **you should change it**. Guidance on creating a strong password can be found on the **Cyber Aware** website.



### MANAGING YOUR ACCOUNT

- To **set-up and manage your device**, you may need to create or use an existing account on the manufacturer's website. This account may allow you to add a new device or link your smartphone to your devices. You should ensure that your account has a **strong password**.
- For added security, if the device or app offers **Two Factor Authentication** which provides a second layer of security, (such as a text message to your phone) you should enable it. This is particularly important if the account contains your **personal data** or **sensitive information** or is linked to something that may impact your or another person's physical safety.
- **Some products allow you to access or control them** when you are away from your home's Wi-Fi network; such as, to view security camera footage. Consider whether you need to make use of this feature, as products may allow you to disable it either in the app settings or within your account.



### KEEP UPDATING YOUR SOFTWARE AND APPS

Much like your laptop and smartphone, software and app updates help keep your devices secure. You should:

- **Check whether you can set-up and enable automatic updates** (on the app or on your online account).
- **Install the latest software and app updates**. These updates should download and install automatically on your device. If not, then you should install them straight away so you have the latest security protections. You should be prompted when a new update is ready to install, usually via a pop-up message or in the settings menu in the app or device menu.



### IF YOU BECOME AWARE OF AN INCIDENT AND THINK IT AFFECTS YOUR DEVICE

- **Visit the manufacturer's website** to see if there is information available on what you should do next.
- Check the **National Cyber Security Centre** and the **Information Commissioner's Office** websites to see any published guidance.
- Further advice on your consumer rights can be found on the **Which?** and **Citizens Advice** websites.



Department for  
Digital, Culture,  
Media & Sport



HM Government



[www.cyberaware.gov.uk](http://www.cyberaware.gov.uk)



# Labelling

- Evidence based research on an IoT label based on priority aspects of the Code and ETSI TS
- Engaging with international governments and expert working group
- Reviewing how and where labels are signposted to consumers
- Further details on labelling scheme in Spring 2019



# Resources

- Programme website  
<https://www.gov.uk/government/publications/secure-by-design>
- IoT Security Mapping  
<https://iotsecuritymapping.uk>
- ETSI TS Cyber Security for Consumer Internet of Things (DTS/CYBER-0039) (ETSI TS 103 645)  
[https://portal.etsi.org/webapp/WorkProgram/Report\\_WorkItem.asp?wki\\_id=54761](https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?wki_id=54761)
- Secure by Design blog on detail and context  
<https://dcmsblog.uk/category/digital/>



# Apply your knowledge!

- Next week you should:
  - Read the Code of Practice and understand where you are in the ecosystem
- In the first three months you should:
  - Assess any IoT products you control, manufacture, sell or use
  - Understand who the key stakeholders are – e.g. mobile app providers, device suppliers etc.
- Within six months you should:
  - Understand how the security of these IoT products and services maps to existing recommendations and standards





# RSA<sup>®</sup>Conference2019

## Thank you!

[david.rogers@culture.gov.uk](mailto:david.rogers@culture.gov.uk)



[@drogersuk](https://twitter.com/drogersuk)