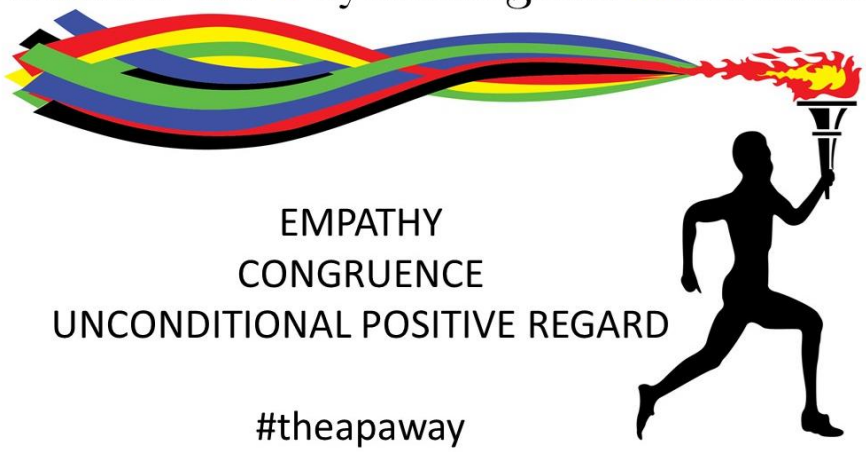
Association for Psychological Accreditation

Association for Psychological Accreditation



Home of The International Psychological Standards & Accreditation Council

APA's Protection Advice:

Risk of External Manipulation of Digital Devices

Overview

All devices capable of receiving or transmitting electrical or digital signals are increasingly vulnerable to external manipulation. Advances in connectivity, smart technology, and remote access capabilities have created new security risks that affect both personal and professional environments.

Devices that were once considered low risk are now potential entry points for unauthorised access, surveillance, or data compromise.

Devices at Risk

The following commonly used devices may be susceptible:

- **Mobile phones**
- **Smart TVs**
- **Laptops and tablets**
- **Digital access devices** (e.g., voice assistants such as Alexa, Siri, etc.)
- **Smart home appliances**, including:
    - Digital vacuum cleaners
    - Smart speakers
    - Connected cameras
    - IoT-enabled household devices

Even devices not traditionally associated with data storage or communication can now be exploited due to embedded connectivity features.

Key Risks

Compromised devices may lead to:

- Unauthorised location, audio or video surveillance
- Data theft or leakage
- Remote device control
- Network infiltration (using one device to access others)
- Exposure of sensitive client or professional information

This presents a **clear and present risk** to:

- Confidentiality
- Personal safety
- Professional integrity
- Organisational security

Risk Mitigation Guidance

To reduce exposure and improve security, the following measures are strongly recommended:

1. Device Management

- Keep all devices updated with the latest software and security patches
- Disable unnecessary features (e.g., microphones, cameras, Bluetooth when not in use)
- Remove or disconnect unused devices

2. Network Security

- Use strong, unique passwords for Wi-Fi networks
- Enable network encryption (WPA3 where available)
- Avoid using public or unsecured Wi-Fi for sensitive activities

3. Access Control

- Enable multi-factor authentication (MFA) wherever possible
- Restrict device access to authorised users only
- Regularly review connected devices on your network

4. Smart Device Precautions

- Mute or power down voice-activated devices when discussing sensitive information
- Avoid placing smart devices in confidential meeting areas
- Review and limit permissions granted to apps and devices

5. Physical Awareness

- Be mindful of device placement in private or professional settings
- Do not assume any connected device is secure by default
- Treat all "always-on" devices as potential listening tools

Final Note

As technology evolves, so do the methods used to exploit it. Vigilance, awareness, and proactive security practices are essential to safeguarding both personal and professional environments.

Reducing risk is not about eliminating technology but about **using it consciously and securely**.

A new approach for new results

Contact us

- By telephone: Call our customer service team on 0208 556 4984
- By email: support@apa-accreditation.co.uk
- In writing: Ayanay Psychological Accreditation,
  11 – 13 Cambridge Park, Wanstead, London E11 2PU