ROYAL HOLLOWAY UNIVERSITY OF LONDON

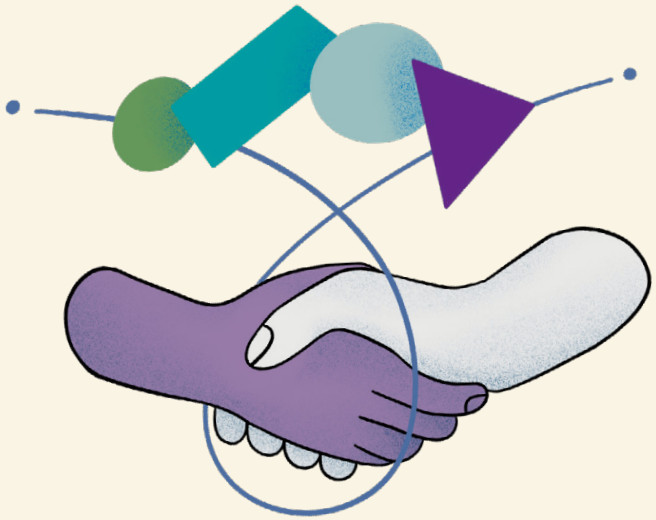
SURREY DOMESTIC ABUSE PARTNERSHIP

Tech Abuse Handbook

The SDAP Tech Abuse Handbook – Your Guide to Digital Safety

Technology, while convenient, is increasingly exploited by perpetrators to cause harm in relationships. Some tech abuse is obvious, but other forms are subtle, hidden in app settings and invisible connections. This handbook, co-developed by the Surrey Domestic Abuse Partnership (SDAP) and Royal Holloway University of London, helps you take back control. It doesn't try to cover everything but focuses on simple steps that can make a real difference.

If any part of this feels unfamiliar, reach out to a trusted, tech-savvy friend or support worker for help. You don't need to do everything at once, and you don't need to do it alone.



Your Digital Safety
The Basics

There are a few simple steps that you can take to protect your online accounts and privacy.

Account Protection

Take time to go through your important accounts one by one – including email, social media, Google or Apple ID, online banking, shopping accounts, health and fitness apps, cloud storage, streaming services (e.g. Netflix), and smart home devices.

Where possible, you can replace existing accounts with brand-new ones.

New Email and Accounts

Set up a new email account that only you can access. Services like ProtonMail are free and let you create an account without using personal details or a phone number. Your new email address can be used to set up all other accounts (e.g. social media and banking) securely.

Strong Passwords

Use new passwords that are hard for others to guess, for example, based on a combination of three random words like “PurpleTeacupGarden”.

For devices only you can access, you can use a free password manager like Bitwarden to generate and save unique passwords for all your accounts.

Two-Factor Authentication (2FA)

For extra security, enable 2FA. Even if someone has your password, they can't log into 2FA-protected accounts without your phone. Install an app like Google/Microsoft Authenticator or Authy to get started.

Protecting Your Existing Accounts

Instead of creating new accounts, you can also review the settings of your existing accounts. Note that changing certain settings (like your recovery email or phone number) may trigger a notification to the old contact details. If someone else has access to those, they may be alerted to your actions. Only make the following changes if you feel it's safe to do so.

- Change passwords to new and strong ones.
- Set a new secure email as the account/recovery email.
- Remove any (recovery) phone numbers you don't fully control.
- Update security questions using answers that no one else would know; you can even use fake answers if that feels safer.
- Log out all active sessions and devices – not just the one you're using – to prevent access to your accounts from elsewhere.
- Unlink any connected accounts that may give someone hidden access.
- Optional: Turn on two-factor authentication (2FA).

Privacy Protection

The following steps help you to prevent personal information from being used to track, monitor, or harm you.

Careful Data Sharing

Avoid posting updates on social media or in WhatsApp status. Consider removing old posts or photos that reveal your location, routines, or relationships. Ask friends and family not to post pictures, tag you, or mention your location online.

Privacy Settings

Many apps share more about you than you realize. Go through your accounts and change who can see your profile, pictures, and posts. Adjust settings so your “last seen” or location isn’t visible. You can usually change these to “Only Me” or “Private”.

Account Deactivation

If necessary, deactivate your accounts and then uninstall apps for peace of mind.

Search for Yourself Online

It’s a good idea to search for your name or username on sites like Google to see what comes up. You can also search your pictures online to check for unauthorised use. If you find something that shouldn’t be there, you can usually report it to the platform for removal.

For Parents

Children's accounts and devices (e.g. tablets, Xbox, Nintendo Switch) can be misused to track, monitor, or cause harm. Protecting them helps keep both your child and yourself safer online.

Apply general Account and Privacy Protection measures

The same protections you use for your own accounts (strong passwords, secure recovery options, and strict privacy settings) can also be applied to your child's accounts and devices.

Review Friend Lists and Chats

If necessary, go through your child's contacts in apps and games. Remove anyone that both of you don't recognise and turn off features that allow strangers to message your child.

Turn Off Location Sharing

Many apps and games let users share their location. Disable such features so no one can track your child's movements.

Look for Extra Accounts on Devices

On tablets and gaming consoles, check if there are "family", "guest", or admin accounts you didn't set up. Remove any that could give someone hidden access.

Financial Abuse

"It wasn't just about money; it was about control, about making me utterly dependent."

Risk Examples

Stopping Your Access to Money

Someone blocks you from using your own bank account, cards, or financial apps – or redirects money like benefits or child support so you can't access it.

Monitoring Your Spending

Every transaction is monitored – you may be questioned, judged, or even punished for how you spend money, no matter how small the amount.

Misusing Your Personal Information

Your personal details are used without your consent – for example, to apply for credit, claim benefits, or register things in your name – which can lead to long-term legal or financial problems.

How to Protect Yourself

- **Open a new bank account in your name only** to prevent access to your financial resources through a joint account, family links, or legal relationships like marriage.
- **Turn on transaction alerts** by going into your online banking settings, usually under “notifications” or “security alerts”, to monitor any account activity in real time.
- **Check your account statements regularly** for unfamiliar or suspicious transactions.
- **Monitor your credit score** (e.g. via Credit Karma or Experian) to look for loans, credit cards, or accounts opened in your name without your knowledge.
- **Contact your bank’s support team if you spot anything concerning** – many UK banks offer specialist help and safe spaces in branches for those affected by financial abuse.

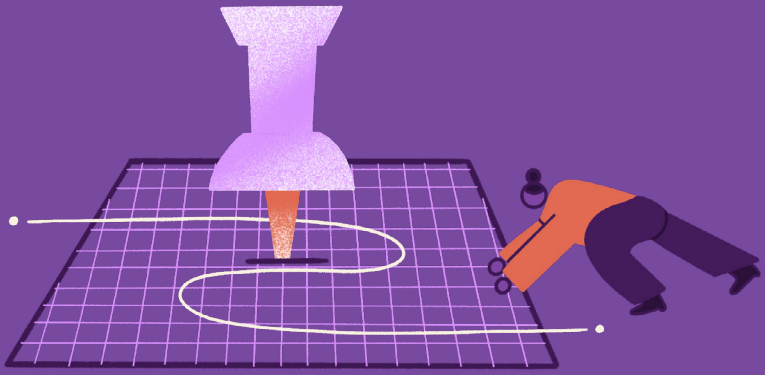
Additional Resources

Surviving Economic Abuse:

Women’s Aid Long-Term Support:

Example of Secure Banking:

Government Advice:



Location Tracking

Risk Examples

Spyware

Hidden apps may be installed on your phone, tablet, or computer – letting someone track your location, access your camera or microphone, see your screen, or record what you type, including passwords.

Hidden Trackers

Small tracking devices, like AirTags or Bluetooth tags, can be slipped into bags, pockets, or hidden in your car.

Misusing Location Apps

Legitimate apps like “Find My”, Google Maps, Snapchat, or even fitness apps can be used to track your movements – often through shared or connected accounts, or settings you didn’t realise are active.

Smart Device Spying at Home

Smart home devices (like doorbell cameras, smart speakers, or even your Wi-Fi router) can be used to monitor when you’re home and who visits.

How to Protect Yourself

- **Turn off location services** for any app that doesn't absolutely need it, through your phone's privacy or settings menu.
- **Check apps like "Find My", Google Maps, Snapchat, or fitness trackers for location history** or live sharing and turn these features off.
- **Scan for spyware**; on Android, you can use apps like Incognito Spyware Detector; on iOS, run a Safety Check under Settings -> Privacy & Security to review who has access to your information.
- **Physically check your bag, coat, car, and personal items** (like stuffed toys or keyrings) for hidden trackers; if you're unsure about your car, ask a trusted mechanic or a service like Halfords to check for tracking devices during a routine check-up.
- **To detect Apple AirTags, use an iPhone's "Find My" app** or download the free Tracker Detect app on Android to scan for nearby trackers not registered to you.

"They hid an AirTag in my kid's backpack and another in my car. It's like we can't go anywhere without being followed."

Additional Resources

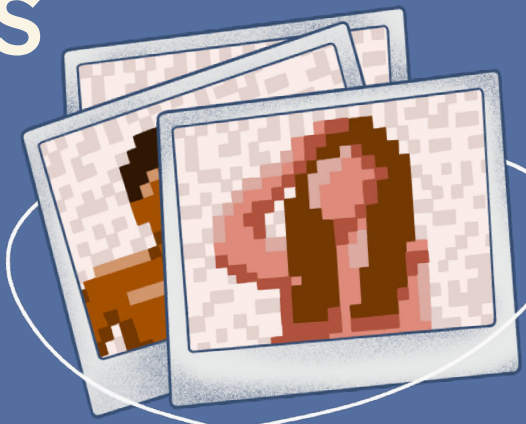
Location Settings (iOS):

Location Settings (Android):

Finding Car Trackers:

Tracking Prevention:

Intimate Images & Videos



Risk Examples

Being Pressured to Send Intimate Images

Someone may force, manipulate, or threaten you to send intimate images or videos.

Non-Consensual Sharing with Others

Intimate images of you are passed around, posted online, or shown to others without your consent.

AI-Generated or Fake Images

Someone uses AI tools to create fake or manipulated sexual content using your face or body to humiliate, impersonate, or frame you.

Blackmail

You're threatened with the release of intimate images unless you do what the perpetrator demands.

“He forced me to send photos, then shared them without my OK. And now with AI, they can even make fake ones. It’s like my own body isn’t mine anymore.”

How to Protect Yourself

- **Report any non-consensual sharing of intimate images** using tools like StopNCII.org and the reporting options on social media platforms and search engines.
- **You can even proactively create a case on StopNCII.org** – this lets you securely submit digital fingerprints of your intimate images so platforms can block them before they’re ever shared online.
- **Save any evidence of threats or image-based abuse**, in case you need to report it to the police or a platform later.
- **If AI-generated (“deepfake”) images of you appear online, report them as image-based abuse** – UK law increasingly treats these like other non-consensual intimate images, and platforms are required to remove them.
- **Avoid creating or sharing new intimate images or videos.**

Additional Resources

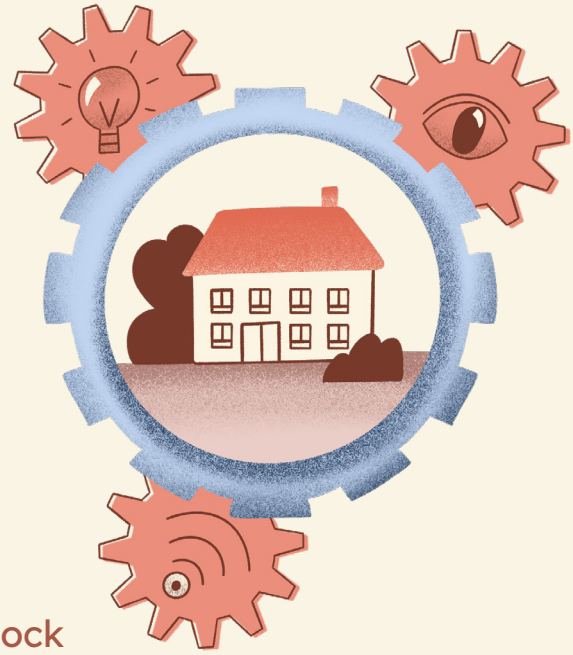
Image/Video Reporting:

Revenge Porn Helpline:

Image/Video Reporting (<18y):

Police Advice:

Smart Home



"My smart home became a trap. He'd lock me out, mess with the heating, and I knew the cameras were always watching and listening. My own home felt like it was spying on me."

Risk Examples

Being Locked Out or Trapped Inside

Someone uses smart locks or alarm systems to prevent you from getting into your home – or to stop you from leaving.

Disrupting Your Home Environment

Lights, TVs, speakers, heating, or other appliances may be turned on, off, or manipulated remotely to confuse, frighten, or make you feel uncomfortable.

Being Watched or Listened to

Smart speakers, cameras, or hidden microphones are used to secretly listen to your conversations or watch what you're doing at home.

How to Protect Yourself

- **Remove the perpetrator's access** by deleting their user accounts or logged-in sessions from smart home apps like Amazon Alexa, Google Home, Apple HomeKit (Home app), Ring, Nest, SmartThings, or Hue.
- **Use a free network scanning app** like Fing to see all devices connected to your Wi-Fi – this can help reveal hidden cameras, microphones, or tracking devices.
- **Scan for nearby Bluetooth devices** in your phone's Bluetooth settings to spot suspicious devices that may be tracking or listening nearby.
- **Change your Wi-Fi password** to stop any devices set up by the perpetrator from staying connected – you can usually do this by logging into your Wi-Fi access point (check the sticker on the access point for details or contact your internet provider for help).
- **Reset all smart devices** (like connected cameras, thermostats, smart meters, or digital door locks) to factory settings or unplug them completely if you don't strictly need them.

Additional Resources

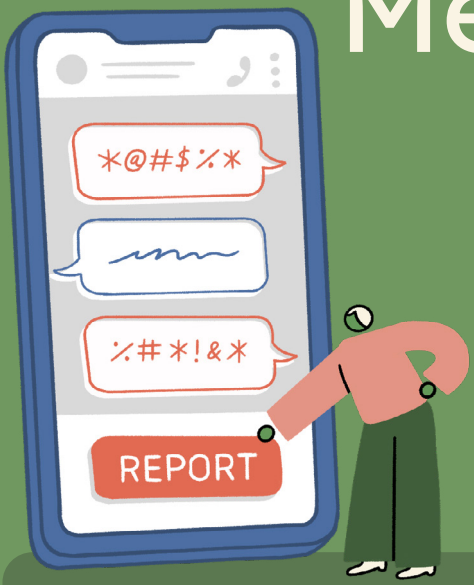
Amazon Echo Security:

WiFi Security:

Ring Security:

Smart Home Security:

Messaging Apps & Social Media



Risk Examples

Being Controlled Through Messaging

You may be pressured to constantly check in or reply right away, or have messages used against you in group chats to create drama or isolate you from others.

Having Your Online Life Monitored

Someone might track your “last seen” status, obsessively monitor your posts and friends/follower lists, or even stalk your contacts (e.g. their location on Instagram) to keep tabs on you.

Harming Your Reputation or Career

Fake (potentially AI-generated) or compromising content might be posted to shame you publicly, or someone may interfere with your emails, job applications, or professional contacts to block opportunities.

Location Tracking Through Social Media

Posts, photos, tags, or check-ins on apps like Snapchat or TikTok can be used to figure out or confirm where you are, even if you didn’t mean to share your location.

“They controlled my messages, watched my every post, and even messed with my job. It felt like my whole digital life became a way to track and trap me.”

How to Protect Yourself

- **Adjust your privacy settings** to limit who can see your profile, contact you, view your posts, or check your “last seen” status – most platforms allow you to set everything to “Private”.
- **Avoid responding to abusive messages.**
- **Save messages or take screenshots as evidence.** Be aware that some apps send notifications when you take a screenshot.
- **Use the platform’s built-in tools** to report harassment, threats, or impersonation – reporting can often be done without the other person knowing.
- **Consider muting or blocking the perpetrator** and any accounts linked to them, including friends or fake profiles – but only if you’re confident it won’t escalate the situation.

Additional Resources

Instagram Reporting:

TikTok Reporting:

Facebook Reporting:

Government Reporting:

SURREY
DOMESTIC ABUSE
PARTNERSHIP

The Surrey Domestic Abuse Partnership – a group of four charities working together to support survivors across the county and build a future free from domestic abuse.

North Surrey Domestic Abuse Partnership

01932 260690
outreach@nsdas.org.uk
www.nsdas.org.uk

East Surrey Domestic Abuse Service

01737 771350
support@esdas.org.uk
www.esdas.org.uk

South West Domestic Abuse Service

01483 898884
swr@swsda.org.uk
www.swsda.org.uk

Your Sanctuary

01483 776822
outreach@yoursanctuary.org.uk
www.yoursanctuary.org.uk

If we're closed, you can still get help:

Your Sanctuary helpline on **01483 776822** is open Mon–Fri between 9am and 9pm

Our Online Chat at **www.yoursanctuary.org.uk/onlinechat** is open Mon–Fri between 9.30am and 5pm

24-hour National Domestic Abuse Helpline: **0808 2000 247**

In an emergency, always dial **999**

For non-emergencies, call **111**

A collaboration between the Surrey Domestic Abuse Partnership (SDAP) and the Information Security Group (ISG) at Royal Holloway, University of London (RHUL).

Funded by the RHUL Social Science Impact Accelerator (SSIA).

Disclaimer: The quotes used throughout this handbook are fictional but inspired by real experiences. Some advice provided in this handbook might be contrary to general cyber security best practice; applicability depends on personal circumstances in tech abuse situations.

This version of the Tech Abuse Handbook was published in November 2025.