



Travel Technology: What to Carry, What to Leave Behind

A practical guide to travelling with the right devices — and none of the ones that create more risk than value.

Technology can make business travel easier, safer, and more productive. It can also add unnecessary weight, attract attention, expose sensitive information, and leave travellers dependent on equipment they don't fully understand.

The aim isn't to carry every possible device. It's to take the minimum technology needed to complete the journey safely and effectively.

Start With the Purpose of the Trip

Before packing, work out what the traveller will actually need to do:

- Access to company systems?
- Video calls, presentations, or large files?
- Poor mobile coverage or unreliable electricity at the destination?

A short trip of meetings might need little more than a phone and a lightweight laptop. A longer assignment, remote site visit, or higher-risk journey may justify extra power, communications, and backup equipment. Technology should support the itinerary, not complicate it.

What to Carry

- **A reliable mobile phone** — usually the single most important item, covering communications, navigation, bookings, translation, banking, identity verification, and emergency contacts. Update fully before departure, protect with a strong passcode, and check international roaming or use an approved local SIM/eSIM. Store important contacts offline too.
- **A laptop, only when required** — don't carry one automatically. If secure access is possible through a managed tablet or phone, leave it behind. When needed, it should be encrypted, updated, and protected by multifactor authentication, holding only what the trip requires. Consider a clean, travel-only device for higher-risk destinations.
- **A compact charging kit** — one reliable multi-port charger, the necessary cables, a travel adaptor, and a spare cable for the most important device. Skip cheap, damaged, or unbranded chargers.
- **A power bank** — useful for long journeys, delays, site visits, or unreliable electricity. Big enough for a demanding day, not so big it's a burden. Carry in hand luggage and check airline rules first.
- **Secure headphones or a headset** — improves privacy and comfort. Remember: headphones give acoustic privacy, not visual privacy — avoid sensitive conversations where screens can be seen or calls overheard.

- **Offline access to essential information** — flight and hotel details, local contacts, emergency and assistance information, copies of travel documents, meeting addresses, transport arrangements, and destination guidance, stored securely.
- **A small backup for critical journeys** — for longer, remote, or higher-risk trips, a simple backup phone provides a second means of communication if the primary is lost, damaged, stolen, or locked. Charge, test, and confirm it works at the destination first.

What to Leave Behind

- **Unnecessary personal devices** — extra tablets, smartwatches, cameras, gaming devices, and secondary laptops add weight and exposure. If it serves no clear purpose on this trip, leave it home.
- **Devices holding excessive data** — don't carry years of emails, client records, or sensitive files just because the laptop has them. The less carried, the less exposed.
- **Unknown USB drives** — easily lost and a common malware vector. Use only encrypted, organisation-approved storage, and never connect an unidentified drive to company equipment.
- **Cheap public charging cables and stations** — public USB points can be a security risk. Use your own charger with a direct power socket, or a power-only USB adaptor if unavoidable.
- **Smart devices that reveal more than they should** — luggage trackers, fitness devices, and watches can expose location, routines, and personal details. Check rules in advance — some secure facilities prohibit connected devices entirely.
- **Equipment that draws attention** — high-value or specialist gear invites unwanted interest, and communications equipment can raise questions at customs or checkpoints. Carry what's needed, pack it discreetly.

Prepare Devices Before Departure

Devices should be updated with current security patches, backed up, encrypted, protected with strong passcodes, set up with multifactor authentication, configured to lock automatically, cleared of unnecessary sensitive information, running approved security software, and able to be located or wiped remotely where appropriate.

Test before you travel: chargers, adaptors, roaming arrangements, and authentication methods. Finding out an account needs a code sent to a UK SIM that doesn't work abroad is an entirely avoidable way to start a trip badly.

Use Technology Carefully During Travel

- Avoid discussing sensitive matters in public, or displaying confidential information on a visible screen
- Never leave devices unattended
- Treat public Wi-Fi with caution; use an approved VPN where required
- Turn off Bluetooth, file sharing, and automatic connection features when not needed
- Keep devices in hand luggage and stored securely in hotels, vehicles, and meeting locations

Consider the Destination

Technology requirements should reflect local conditions. Some countries restrict satellite communications, drones, encrypted equipment, cameras, or certain mapping apps, and border officials may have the power to inspect devices. Electricity, mobile coverage, and secure internet access can all vary significantly by location.

For higher-risk travel, decide in advance what equipment can be carried, what data can be accessed, and what the traveller should do if a device is examined, lost, or compromised.

After the Journey

Devices used on higher-risk trips may need checking before reconnecting to company systems. Travellers should report unusual login requests, suspicious messages, lost equipment, or unexpected changes in device behaviour — and passwords may need changing, temporary accounts closing, and travel-only devices resetting. Post-travel checks should be proportionate to the destination and the information accessed.

Quick Reference Checklist

Before departure, confirm:

- ☐ Devices limited to what this trip actually requires
- ☐ Phone and laptop updated, encrypted, and passcode/MFA protected
- ☐ Charging kit consolidated — no unnecessary plugs or cheap cables
- ☐ Power bank packed in hand luggage, airline rules checked
- ☐ Essential information saved offline and stored securely
- ☐ Backup communication method arranged for higher-risk trips
- ☐ Destination restrictions on equipment and data checked in advance
- ☐ Post-travel device and password checks scheduled if required
- ☐ Burner phone, privacy screen, or cable lock packed if the trip warrants them

Physical Security Add-Ons

A few low-cost items add a physical layer of protection alongside the digital precautions above:

- **A burner phone** — a basic, unlocked device (a simple 4G feature phone, or a low-cost Android if apps like Maps and banking are needed) bought separately from the traveller's main phone and loaded only with what the trip requires. No synced accounts, no personal history. Ideal for higher-risk destinations or where a lost or seized phone shouldn't expose anything beyond the trip itself.
- **A laptop privacy screen** — a magnetic clip-on filter matched to the laptop's exact screen size and aspect ratio. It blocks side-on viewing in airports, lounges, and shared workspaces without permanently dimming the screen, and comes off in seconds when not needed.
- **A cable lock** — a Kensington-style security cable that loops around a fixed object and into the laptop's lock slot (check whether the device uses a standard, nano, or wedge-shaped slot before buying). A combination lock avoids the risk of losing a separate key, and it's most useful for the moments a laptop has to be left briefly — a conference hall, a shared workspace, a hotel breakfast table — rather than a substitute for keeping it with you.

None of these replace judgement: a burner phone, privacy screen, or cable lock reduce specific risks — they don't substitute for keeping devices attended, encrypted, and limited to what the trip actually needs.

Carry Less, Prepare Better

Good travel technology isn't about owning the latest equipment. It's about choosing reliable devices, reducing unnecessary exposure, and making sure the traveller can communicate, work, and get support when normal arrangements fail.

The strongest kit is usually simple: a secure phone, the right business device, dependable power, essential information, and a tested backup plan.

Initiative Training Group helps organisations strengthen travel preparation, traveller security, and digital risk arrangements as part of a structured travel risk management programme.

Carry what the journey requires. Leave behind what creates more risk than value.

☎ +44 1432 818999 ✉ info@initiativetraininggroup.com