Digital Safety & Governance Meeting Checklist

Use this at quarterly meetings, after major life changes, or whenever a new device, adviser, account, household member, or employee's role is added.

This checklist reframes personal online safety controls into a governance format built for shared decision-making across advisors and generations. It is organized around five questions: What are we exposing? Who can get in? Who can act? How do we verify? Who responds?

Priority actions to confirm now

- ☐ Turn on passkeys, security keys, or other phishing-resistant multifactor authentication on priority accounts wherever possible.
- ☐ Use a password manager and unique long passwords for every account.
- ☐ Confirm that each adult in the household has credit-file protections in place where relevant, such as a freeze at all three bureaus in the US.
- ☐ Put tax-account safeguards in place where relevant, such as an IRS Identity Protection PIN (IP PIN) in the US or the strongest available identity protection through the applicable tax authority account.
- ☐ Use a callback protocol for wires and other sensitive changes, and turn on real-time alerts for new payees, logins from new devices, password changes, and large transactions.
- ☐ Review the Personal Online Safety Checklist for additional preventive actions and incident-response steps.

Meeting date	_____	**Next review date**	_____
Facilitator / note-taker	_____	**Participants / households represented**	_____

Roles to confirm for this cycle

Digital lead	Finance verifier	Incident contact	Next-gen support lead	Outside adviser / IT contact

How to use this checklist

Work through the sections together. Mark completed items, identify gaps, assign owners, and record only the next few actions that truly matter before the next meeting. Include senior and rising-generation voices; the goal is not perfect technical fluency, but clear roles, normal verification, and steady follow-through.

1. Awareness

Core question: *What are we exposing?*

- ☐ Review the digital footprint: personal email, financial accounts, tax and government accounts, shared drives, household systems, phone plans, password managers, home-network devices, and any platforms used by assistants or advisers.
- ☐ Ask what changed since the last meeting: new phones, laptops, service providers (e.g., mobile carriers), employees, advisers, schools, travel plans, entities, trusts, or homes.
- ☐ Check whether emails or phone numbers appear in known breaches and note any reused passwords that still need to be changed.

- ☐ Review the public footprint: social media profiles, travel-posting habits, exposed addresses, people-finder sites, and Google search results that could support impersonation or credential reset.
- ☐ For children and young adults, confirm who is monitoring identity exposure and whether appropriate credit safeguards are in place, such as a child credit freeze in the US where applicable.

Cross-generational discussion prompt

Have each generation name one digital habit that feels normal to them but may look risky to someone else in the family. Use that contrast to spot blind spots without blame.

2. Access

Core question: *Who can get in?*

- ☐ Turn on passkeys, security keys, or other phishing-resistant multifactor authentication on priority accounts wherever possible, starting with email, Apple/Google/Microsoft accounts, banks, brokerage, and password managers.
- ☐ Use a password manager and unique long passwords for every account; stop sharing passwords by text, email, or handwritten notes that circulate loosely.
- ☐ Review account-recovery paths: backup codes, recovery email addresses, recovery phone numbers, and spare security keys should be current, secure, and known to the right people.
- ☐ Add carrier port-out or number-lock protection and reduce reliance on SMS codes where stronger options are available.
- ☐ Confirm device basics across generations: automatic updates, full-disk encryption, secure backups, and a hardened home Wi-Fi/router setup with connected home devices isolated when practical.
- ☐ Remove stale access for former employees, ex-advisers, old devices, unused apps, unnecessary browser extensions, and anyone who no longer needs administrator rights.

Cross-generational discussion prompt

Identify who needs setup help, not just policy reminders. Pair confident users with family members who want support getting passkeys, a password manager, or account recovery configured correctly.

3. Authority

Core question: *Who can act?*

- ☐ Define exactly who may approve payments, add new payees, change standing instructions, reset credentials, add trusted devices, or speak for the family with institutions and advisers.
- ☐ Separate support from authorization. A person may help with scheduling, travel, records, or bill preparation without having the right to move money or change account ownership or recovery settings.
- ☐ Document who is the primary decision maker and who serves as backup if that person is traveling, ill, unreachable, or no longer able to act.
- ☐ Confirm where key records live: contact sheet, account inventory, recovery instructions, estate or fiduciary contacts, and escalation paths for banks, service providers, advisers, and insurers.
- ☐ For higher-risk situations, consider extra segmentation such as a dedicated device or phone number for financial activity or tighter protections on accounts with outsized consequences.

Cross-generational discussion prompt

Ask: “If the most senior decision maker could not respond for 48 hours, what decisions would stall, and who is prepared to step in?”

4. Authenticity

Core question: *How do we verify?*

- ☐ Adopt a norm that urgent requests for money, gift cards, crypto, new payment details, or account changes are never acted on from one message or one call alone.
- ☐ Use a callback protocol for bank transfers, wires and other sensitive changes: verify through a known phone number or second trusted channel, not the contact information contained in the request itself.
- ☐ Treat caller ID, voice messages, video calls, QR codes, parcel or parking notices, unexpected Google Docs invites, and "support" calls from banks or technology companies as untrusted until independently confirmed.
- ☐ Agree on which channels are appropriate for sensitive instructions and which are only for convenience or low-risk coordination.
- ☐ Practice making verification normal rather than awkward: no one should feel embarrassed for slowing down a request that feels urgent, emotional, or slightly off.

Cross-generational discussion prompt

Run one short scenario out loud: a cloned-voice call from a relative, a spoofed email changing payment or transfer instructions, or a text from "bank support." Ask each person what they would do first.

5. Action

Core question: *Who responds when something goes wrong?*

- ☐ Create a short incident playbook that names who freezes cards or credit, who contacts institutions, carriers or service providers, who changes passwords, who documents the event, and who coordinates outside help.
- ☐ Make sure the advisor or family knows the first steps for the most likely events: lost device, suspicious payment request, password exposure, phone-number hijack, national ID number exposure (e.g., SSN in the US or NI number in the UK), child identity theft, or a breach notice from a provider.
- ☐ Confirm that adults have the core identity-protection steps handled where relevant: credit-file protections or fraud alerts, tax-account safeguards (e.g., IRS Identity Protection PINs in the US or Government Gateway User ID in the UK), and other secured government accounts (e.g., Social Security).
- ☐ Turn on real-time alerts for new payees, logins from new devices, password changes, and large transactions on financial accounts.
- ☐ Schedule an annual tabletop exercise or brief drill so the response plan is practiced, not theoretical.

Cross-generational discussion prompt

Ask: "Who owns the first 30 minutes?" The right answer should be clear enough that even a teenager or older relative could tell you how the family would respond.

Annual deep-dive and special-event triggers

Add a longer review at least once a year. Also meet outside the normal cadence after a death or incapacity, a major payment or liquidity event, a home purchase or sale, a divorce, a change in advisers or household employees, extensive travel, or a meaningful breach or fraud scare.

- ☐ Review adult and child credit protections where available, tax-account protections, and online government account security where applicable.
- ☐ Check real-time alerts on financial accounts, update trusted contacts, and confirm the bank-transfer callback protocol still matches current advisers and institutions.
- ☐ Review breach alerts for emails and domains, rotate reused passwords, and confirm backup recovery materials (backup codes, recovery contacts, spare security keys) are current.

☐ Revisit public-footprint reduction: people-finder opt-outs, old social media accounts, exposed addresses or travel habits, and public information that could support impersonation.

☐ For families with employees, entities, trusts, philanthropy, or multiple households, review role separation and remove stale permissions across all systems.

Priority follow-ups before the next meeting

Action item	Owner	Due date

Key Contact Information

Type	Contact Name	Email	Phone Number
Brown Advisory Contact			
Banking			
Accounting			
Legal			
Family Employee			