Cyber Seeds Family Pack

Your home is digital. It just hasn't been mapped yet.

The Cyber Seeds Family Pack is a calm, trauma-aware guide to understanding and strengthening your household's digital life. It draws from the Cyber Seeds canon, the Domestic Cyber Standard (DCS-UK) and the six-volume master textbook to offer practical actions that reduce risk and promote wellbeing. This pack is non-judgemental: it is a map, not a score. It is designed for parents, carers, grandparents and anyone who wishes to nurture safer, kinder online habits at home.

How to use this guide

Start with what feels manageable. Each section focuses on one of the **Five Lenses** of household digital ecology. Within each lens you will find a short explanation, a handful of high-impact practices, and gentle suggestions for today, this week and this month. You don't need technical skills; small, repeatable rituals make the biggest difference.

> **Principles of Cyber Seeds:** Safety without shame • Behaviour is infrastructure • Children require special protection • Simplicity over complexity • Public inclusion • Evidence, renewal & accountability • Ethical stewardship.

The Five Lenses of Household Digital Ecology

The Domestic Cyber Standard organises household safety into five overlapping lenses. Working through each lens in turn helps you build resilience one layer at a time.

1. Network & Wi-Fi Safety

The router is your home's digital front door. Strengthening it protects everything behind it.

- Change default admin usernames and passwords on your router and modem.
- Enable the strongest encryption supported (WPA3 or at least WPA2) and disable unused services such as WPS and UPnP.
- Update router firmware regularly and turn on automatic updates if available.
- Create a separate guest network for visitors and isolate children's devices on their own

network if possible.
- Place your router centrally in the home for better coverage and reduced interference.

Today: Locate your router's manual (or search its model online) and change the admin login and Wi-Fi password. Write the new credentials in a secure place.

This week: Log in to the router interface, update the firmware, and enable WPA2/3 encryption. Review the list of connected devices and remove anything you don't recognise.

This month: Set a reminder to check for router firmware updates and schedule a quarterly "network health check" with your family.

2. Device Hygiene & App Safety

Every phone, tablet, laptop, smart-TV or smart-speaker is a potential entry point. Healthy devices reduce the spread of digital weeds.

- Keep operating systems, apps and firmware up to date.
- Use passcodes, biometric locks or passwords on all devices. Turn on automatic screen locks.
- Enable multi-factor authentication for important accounts and install a reputable password manager.
- Review app permissions and uninstall apps you no longer use.
- Back up important data to both cloud and local storage.

Today: Choose one device and run all available software updates. Turn on automatic updates if possible.

This week: Set up a password manager and enable multi-factor authentication on your primary email and financial accounts.

This month: Audit the apps on each family member's devices and remove any that are unnecessary or risky. Encourage children to ask before installing new apps.

3. Privacy & Identity Exposure

Our identities are scattered across services. Managing them reduces the risk of data exploitation.

- Share the minimum personal information online and opt out of data broker lists where

possible.
- Use unique, strong passwords for every account; a password manager makes this manageable.
- Set privacy controls on social media to “Friends only” and review tagged posts and photos.
- Create separate email addresses for high-risk accounts (banking) and general subscriptions.
- Learn about your rights under GDPR and data protection law.

Today: Enable two-factor authentication on your primary email account and bank. Check whether your email appears in any known data breaches via trusted services.

This week: Review privacy settings on social platforms. Remove old posts, photos or tags that reveal sensitive information.

This month: Map your family’s online accounts. For each account, note whether you have strong passwords and 2FA enabled. Close accounts you no longer need.

4. Scam-Prevention & Digital Behaviour

Scams exploit urgency and emotion. Practising calm verification habits protects money and mental health.

- Recognise common scam patterns: unexpected requests for money, urgent threats, messages from unknown senders.
- Slow down and verify. If a message seems urgent, call the person or organisation via a known number.
- Establish a family “safety word” used to verify any financial requests.
- Discuss cognitive traps such as authority bias and scarcity, which scammers exploit.
- Report scams to Action Fraud (UK) or the appropriate local authority; share experiences to help others.

Today: Talk to your household about a recent scam story and agree on your family’s safety word.

This week: Practise a scam scenario: send a fake phishing email to each other and see how you respond. Discuss the emotions that came up.

This month: Review your spam and junk mail folders. Educate children and older relatives

about new scam techniques (e.g. AI voice cloning).

5. Children's Digital Wellbeing

Children experience the digital world differently. Align digital habits with developmental needs and emotional safety.

- Designate screen-free zones and times (mealtimes, bedrooms).
- Co-view and co-play: explore games and apps together to understand what your child enjoys.
- Teach children to name emotions and pause before responding online.
- Encourage critical thinking about algorithms and online peer influence.
- Model healthy digital behaviour: your habits shape theirs.
- Create individual accounts or profiles for each child where possible to reduce conflict.

Today: Share one online activity with your child—watch a video together or discuss their favourite game.

This week: Set a new family ritual such as a weekly "digital detox" evening or a tech-free meal. Discuss feelings about screen time.

This month: Reflect on your child's developmental stage and identify one digital challenge they face. Write down three ways you can support them.

Household Digital Snapshot

The Cyber Seeds "snapshot" is a simple self-assessment tool. You can create your own version by answering these questions. Use the table below to note areas that are strong and those requiring attention. There is no pass/fail—this is a signal, not a judgement.

Lens	Questions to ask	Our status	Next seed
Network	Do we know our router model? Have we changed default passwords? Is encryption (WPA2/3) enabled? Are there unknown devices connected?		
Devices	Are our devices up to date? Do we use lock screens? Have we		

Lens	Questions to ask	Our status	Next seed
	backed up important data?		
Privacy	Do we use unique passwords? Is 2FA enabled? Have we checked our social media privacy settings?		
Scams	Do we know common scam signs? Do we verify payment requests? Do we have a family safety word?		
Wellbeing	Do we have screen-free times? Are we talking about emotions triggered online? Do we model healthy habits?		

Further Support & Resources

Cyber Seeds offers more detailed materials for practitioners, schools and councils, including the *Cyber Seeds Canon*, the six-volume master textbook and the Domestic Cyber Standard. For professional guidance or to request an audit, visit cyberseeds.co.uk. If you suspect a child is at immediate risk, contact emergency services. For non-emergency safeguarding concerns, follow your local authority's protocols.