

// E-SAFETY FACT SHEET

Your Digital Footprint

What colleges, employers, and strangers can find – and how to shape it for Students, Teachers, and Parents

Everyone who spends time online leaves a trail: posts, comments, photos, tags, accounts signed up for and forgotten, and records held by companies nobody remembers dealing with. Together that trail is a digital footprint, and by the time a young person applies to college or for a first job, it has usually been accumulating for a decade.

A digital footprint is not only a reputation problem. It is also the raw material for guessing passwords, answering security questions, and impersonating someone convincingly.

This sheet covers what a footprint is made of, how to audit and clean one up, and how to build one that works in a young person's favour rather than against them.

In this document:

- 01 Know the risks
- 02 What can you do?
- 03 Resources and where to get help

1 Know the risks

A. Delete Is Not Delete

Posts can be screenshotted within seconds, reposted, archived by third-party sites, and cached by search engines. Disappearing messages can be captured by a second phone pointed at the screen. Removing something from your own account removes it from your account — not from everywhere it has already travelled. The practical rule is that anything sent to another person is now under their control.

B. What Colleges and Employers Actually Look At

Searching applicants online is routine. Note what is generally being looked for: not embarrassing teenage posts in isolation, but patterns — harassment or slurs, threats, evidence of dishonesty, or content that suggests someone would be a problem to work alongside. A thin or private footprint is rarely held against anyone. A public one full of abuse is. Scholarship committees, sports programmes, landlords, and internship supervisors search too.

C. You Do Not Control All of It

Other people's posts form part of your footprint: tagged photos, group chat screenshots shared onward, a friend's public account showing your face and their location, a sports team roster listing a full name and school. Content posted by parents about children — sometimes years before the child had any say — is part of it too.

D. Aggregation: Small Pieces, Big Picture

No single post gives much away. A school badge in one photo, a hometown in a bio, a team name, a birthday post, a running route, and a family member's surname together identify a person, their address, and their daily routine. Data brokers automate exactly this, compiling and selling profiles built from public records and online activity. Assembling scattered public information into a picture of a person is a recognised technique — and it's the same one investigators and security researchers use professionally.

E. Your Footprint Is Also Your Attack Surface

The details that make a profile feel personal are frequently the answers to account-recovery questions: a pet's name, a first school, a mother's maiden name, a favourite team. They also supply the raw material for a convincing scam message, since knowing real details about someone is what makes an approach believable. Public information is how a stranger arrives already sounding like a friend.

F. Old Accounts Nobody Closed

Forums, games, and apps signed up for years ago still hold data, still carry an old password, and still show an old username that may link to a current one. Abandoned accounts get breached without anyone noticing, and old content resurfaces under a name that is still searchable today.

2 What can **you** do?

Audit your own footprint — 30 minutes, once a year

STEP 01	Search yourself. Your name, name plus town, name plus school, and every username you've used. Use a private window, and check image results too.
STEP 02	Review your own accounts as a stranger sees them — log out and look at your public profile.
STEP 03	Check tagged photos and turn on tag review so you approve tags before they appear.
STEP 04	Close old accounts you no longer use, and remove old posts that no longer represent you.
STEP 05	Fix the reusable details — anything public that could answer a security question should be changed in settings, not just hidden.

For students

- ▶ Apply the **billboard test**: would you be comfortable with this on a billboard, with your name on it, in five years?
- ▶ Keep **school, address, birthday, and routine** out of public profiles. Those four are most of what a stranger needs.
- ▶ Use a **different username** for gaming and casual accounts than for anything attached to your real name. Reused handles link everything together.
- ▶ Post about events **after** they happen, not live. Real-time location is the most useful thing you can give away.
- ▶ Ask before posting photos of friends, and expect the same in return.
- ▶ Anger, private arguments, and group-chat screenshots age badly. Wait an hour before posting anything written while upset.

For parents & caregivers

- ▶ Audit together rather than for them. A search you run *with* a teenager teaches a skill; one you run behind their back teaches secrecy.
- ▶ Think about your own posting. Children inherit a footprint built by adults — school names, birthdays, and photos posted publicly for years.
- ▶ Remove home address and phone number from public profiles and from old marketplace and sports listings.
- ▶ Ask schools and clubs what they publish publicly about pupils, and what the opt-out is.

For teachers & schools

- ▶ Run the audit as a classroom exercise — searching for yourself lands far harder than being warned about it.
- ▶ Teach the aggregation idea explicitly: safe pieces, unsafe picture.
- ▶ Connect it to the application process students care about, and to the fact that a good footprint is an asset, not just an absence of bad ones.

Build one that helps you. A public portfolio, a project write-up, a certification, or a competition placing all show up in a search too — and they are what turns a footprint into an advantage. Start at getintocyberjobs.com.

3 Resources and where to get help

If something harmful about you is already online

STEP 01	Screenshot it first. Capture the content, the username, and the URL before requesting removal — you may need it for a report.
STEP 02	Report it in-platform. Harassment, impersonation, and privacy violations all breach the rules of every major service.
STEP 03	Ask the site to remove it, then request removal from search results — search engines have request forms for personal information such as addresses and ID numbers.
STEP 04	Tell a trusted adult — and for anything involving threats, sexual content, or a minor, go straight to the reporting routes below.

- ▶ **Google “Results about you”** — monitor and request removal of personal contact details from search results: myactivity.google.com/results-about-you
- ▶ **Have I Been Pwned** — check whether an email appears in a known data breach: haveibeenpwned.com
- ▶ **FTC consumer advice** — online privacy, data brokers, and identity protection: consumer.ftc.gov

- ▶ **StopBullying.gov** — documenting and reporting harassment: stopbullying.gov
- ▶ **NCMEC Take It Down** — helps minors anonymously request removal of explicit images of themselves: takeitdown.ncmec.org
- ▶ **NCMEC CyberTipline** — report exploitation of a child: report.cybertip.org · 1-800-843-5678

A note on removal services. Paid “reputation management” and data-broker deletion services vary enormously in what they deliver, and some trade on panic. Do the free steps above first, and check any paid service carefully before handing over data or money.

// Check these before you post

- ▶ Is your school, uniform, or team visible in the background?
- ▶ Does it show where you live, or a street sign near it?
- ▶ Does it reveal where you’ll be, right now?
- ▶ Does it include anyone who didn’t agree to be in it?
- ▶ Does it give away an answer to a security question?
- ▶ Were you angry or upset when you wrote it — and would it still be fine attached to your name in five years?

Nobody gets every one of these right every time — and one slip is not a crisis. Consistency is what a footprint is actually made of.

getintocyberjobs.com · A free resource for K-12 students and teachers across the US.

This fact sheet is for general educational purposes and is not legal advice for any specific situation. If a child is in immediate danger, call 911. To report online exploitation of a child, contact the NCMEC CyberTipline at report.cybertip.org or 1-800-843-5678.