Privacy Checkup

How Safe Is Your Digital Privacy? • A Comprehensive Audit for Ages 10 to 16

Student Name: _____ **Date:** _____

Class / Group: _____ **Teacher:** _____

Your Mission

This worksheet is your **personal digital privacy audit**. You'll check every aspect of your online life (passwords, social media, personal information, device settings, AI interactions, browsing habits, and phone/messaging safety) and score yourself honestly.

Scoring: For each item, check Y (Yes = 1 point) or N (No = 0 points). If you're not sure, check ? and then investigate!

Why this matters: In 2026, the average person has **100+ online accounts**, shares **1.7 MB of personal data per second**, and is targeted by an estimated **4,000+ ads per day** based on their data profile. Your personal data is valuable. Companies spend billions collecting and trading it. Protecting your privacy is protecting yourself.

Password Safety (Score: ___ / 8)

■ I use a **different password** for every important account

Reusing passwords means if one account is hacked, ALL your accounts are compromised. In 2023, there were 2,365 data breaches affecting 343 million victims (ITRC).

■ My passwords are at least **12 characters long**

An 8-character password can be cracked in under 1 hour. A 12-character password with mixed characters takes approximately 34,000 years (Hive Systems, 2026).

■ My passwords include a **mix of uppercase, lowercase, numbers, and symbols**

Each character type increases the "search space" exponentially. A password with only lowercase letters has 26 options per character; adding all types gives 95 options per character.

■ I **don’t use personal information** in passwords (birthday, pet’s name, favourite team)

This information can often be found on your social media profiles, making these passwords guessable through social engineering.

■ Only my **parents/guardians know** my passwords, not friends

Even best friends can accidentally share passwords, or friendships can change. Keep passwords between you and your parents/guardians only.

■ I use **two-factor authentication (2FA)** on all accounts that offer it

2FA adds a second step (like a code sent to your phone) so even if someone steals your password, they still can’t access your account. It blocks 99.9% of automated attacks (Microsoft).

■ I use a **password manager** or a secure system to store passwords

Password managers like Bitwarden (free), 1Password, or Apple Keychain generate and store strong unique passwords so you only need to remember one master password.

■ I have **never shared a password** over text, email, DM, or chat

Messages can be intercepted, screenshotted, or accessed if someone else picks up your phone. Always share passwords in person if absolutely necessary.

Pro Tips:

• Use a **passphrase** instead of a password: “MyDog8Pizza@Midnight!” is long, memorable, and secure

• The strongest passwords are **random**; let a password manager generate them

• Never use common passwords: “123456”, “password”, “qwerty”, and “111111” are still the most-used passwords worldwide

• Change passwords immediately if a website you use reports a data breach. Check **HaveIBeenPwned.com**

Social Media Privacy (Score: ___ / 8)

■ All my social media accounts are set to **Private** (not Public)

Public accounts mean anyone in the world (including strangers, scammers, and predators) can see everything you post. Private accounts limit visibility to approved followers.

■ I only accept friend/follow requests from **people I know in real life**

Fake accounts are common: Facebook removed 2.6 billion fake accounts in just one quarter of 2023. Accepting strangers gives them access to your personal information and photos.

■ My profile does **not show my real location, school name, or home area**

This combination of information makes it possible for someone to find you physically. Never list your school, neighbourhood, or "current city" on public profiles.

■ I don't post photos showing my **school uniform, house, or identifiable landmarks** near my home

Geolocating someone from background details in photos is surprisingly easy. Street signs, shop fronts, and school crests can all reveal your location.

■ Location tagging / geotagging is **turned OFF** on all my posts and photos

Photos can contain hidden GPS coordinates (EXIF data) that reveal exactly where the photo was taken. Turn off location services for your camera and social media apps.

■ I **think before I post**: "Would I be comfortable if my parents, teachers, and future employers saw this?"

The internet is permanent. Even "deleted" posts can be screenshotted, cached by search engines, or archived by the Wayback Machine. Post as if everything is permanent.

■ I **regularly review** my follower/friend list and remove people I no longer know or trust

Over time, you may accumulate followers you've forgotten about. Do a quarterly cleanup.

■ I have **reviewed the privacy settings** on each platform in the last 3 months

Platforms frequently update their privacy settings, sometimes resetting your choices. Instagram, TikTok, Snapchat, and YouTube all have dedicated privacy settings pages.

Pro Tips:

• Review your privacy settings on each platform: **Instagram** > Settings > Privacy; **TikTok** > Settings > Privacy; **Snapchat** > Settings > Who Can...

• Use the "View As" feature (available on Facebook and some others) to see what your profile looks like to strangers

• Be cautious with "Close Friends" or "Best Friends" lists; make sure only genuinely trusted people are on them

Personal Information Protection (Score: ___ / 7)

■ I don't share my **full real name** on public-facing profiles or forums

Use a nickname, username, or first name only. Your full name combined with other details makes identity theft much easier.

■ I **never share my phone number** with people I only know online

Phone numbers can be used for SIM-swapping attacks, harassing calls, or doxxing. Keep your number within your real-life circle.

■ I don't share my **address, postcode, or specific location** with anyone online

Even partial location information can be pieced together. Never share your postcode, street name, or nearby landmarks with online contacts.

■ I **ask a parent/guardian before filling in online forms** with my information

Many forms are designed to collect data for marketing. Adults can help identify legitimate forms vs data harvesting operations.

■ I use a **nickname or username** that doesn't reveal my real name, age, or gender

Avoid usernames like "Sarah2012London" which reveal your name, birth year, and city. Use something unrelated like "BlueRocket42".

■ I know what **personally identifiable information (PII)** is and I protect it

PII includes: full name, date of birth, address, phone number, email, school name, photos of your face, financial information, and biometric data (fingerprints, face scans).

■ I don't participate in **social media quizzes or challenges** that ask personal questions

"What's your rapper name? (First pet + street you grew up on)" These are designed to harvest security question answers. Don't fall for them.

Pro Tips:

• Remember the **Grandma Test**: Don't share anything online that you wouldn't want your grandma (or a stranger) to know about you

• Your email address is personal data too. Consider using a separate email for signing up to websites and newsletters

• Be especially careful with your **date of birth**; it's a key piece of identity data used for verification by banks and services

Device & App Settings (Score: ___ / 8)

■ My phone/tablet has a **passcode, Face ID, or fingerprint lock**

Your device contains your entire digital life. Without a lock, anyone who picks it up has access to your messages, photos, social media, and email.

■ I've **reviewed which apps have access** to my camera, microphone, and contacts

Go to Settings > Privacy on iPhone, or Settings > Apps > Permissions on Android. Many apps request permissions they don't need.

■ **Location services** are set to "While Using the App" or OFF for most apps

Apps that always track your location build a detailed profile of your daily movements. Only maps and weather genuinely need constant location access.

■ I **don't click on pop-ups, suspicious links, or "You've won!" messages**

These are almost always phishing attempts or malware. Legitimate companies don't contact you through random pop-ups.

■ I only download apps from **official app stores** (App Store / Google Play)

Third-party app stores and direct APK downloads can contain malware. Even on official stores, check reviews and developer reputation before downloading.

■ My device's **operating system is up to date**

Updates patch security vulnerabilities. Delaying updates leaves known vulnerabilities that hackers can exploit. Enable automatic updates.

■ I **don't connect to unsecured public Wi-Fi** without a VPN

Public Wi-Fi at cafes, shops, and trains can be monitored. Hackers can intercept your data on unsecured networks. Use mobile data or a VPN for sensitive activities.

■ I have **reviewed and limited ad tracking** on my device

iPhone: Settings > Privacy > Tracking > "Allow Apps to Request to Track" OFF. Android: Settings -> Google -> Ads -> Delete advertising ID.

Pro Tips:

• Do a **permission audit** right now: open Settings and check which apps have camera, microphone, location, and contacts access. Remove any that don't need it

• Turn on **automatic updates** for your device and apps

• Use **Bluetooth and NFC only when needed**. Turn them off when not in use to reduce your attack surface

AI & Chatbot Privacy (Score: ___ / 6)

■ I **never share personal information** (name, age, school, address) with AI chatbots

Conversations with AI chatbots may be stored, reviewed by humans, or used for training. OpenAI, Google, and others state this in their terms of service. Treat chatbots like public conversations.

■ I understand that AI chatbots **can't keep secrets**; my conversations may be stored and reviewed

In 2023, Samsung employees accidentally leaked confidential company data by pasting it into ChatGPT. Never share anything with AI that you wouldn't say publicly.

■ I **don't use AI to make images of real people** without their consent

Creating fake images of real people (especially inappropriate ones) can be illegal and is always harmful. This includes deepfakes of classmates, teachers, or celebrities.

■ I know that **AI-generated content isn't always accurate** and I fact-check important information

AI "hallucinates": it confidently generates false information. In 2023, a US lawyer submitted a legal brief with AI-fabricated case citations that didn't exist.

■ I **don't upload personal photos** to AI image generators or face-swapping apps

Your face is biometric data. Uploading photos to AI services gives them training data and may violate privacy regulations. Some apps store and use your face data indefinitely.

■ I **read the privacy policy summary** before using a new AI tool

Check: What data is collected? Is it shared? Can you delete it? Is it used for training? Reputable AI tools will clearly answer these questions.

Pro Tips:

• When using ChatGPT: Settings > Data Controls > turn OFF "Chat History & Training" to prevent your conversations from being used to train the model

• Never paste **homework assignments, personal essays, or creative writing** into AI if you don't want it to become training data

• Be aware that **voice assistants** (Siri, Alexa, Google Assistant) also collect data; review their privacy settings too

Browsing & Internet Habits (Score: ___ / 6)

■ I check for **HTTPS (the padlock icon)** before entering any personal information on a website

HTTPS encrypts data between your browser and the website. Without it, anyone on the same network can potentially see what you're typing, including passwords.

■ I **don't click on links in unexpected emails or messages**

Phishing emails are the #1 cyber attack method. Even if an email looks like it's from a trusted company, hover over links to check where they actually lead before clicking.

■ I **clear cookies and browsing history** regularly

Cookies track your browsing across websites to build advertising profiles. Clear them weekly, or use browser settings to block third-party cookies.

■ I use a **privacy-focused browser or search engine** (Brave, DuckDuckGo, Firefox with tracking protection)

Standard Chrome with default settings tracks significant browsing data. Privacy-focused alternatives reduce tracking without sacrificing functionality.

■ I **don't click "Accept All Cookies"** automatically; I review and choose

Cookie consent banners are legally required in many countries. Clicking "Reject All" or customising to accept only essential cookies protects your privacy.

■ I know how to **recognise a phishing website** (misspelled URLs, suspicious domains)

Scam sites often use slight misspellings: g00gle.com, amaz0n-login.com, or paypal.secure-login.xyz. Always type important URLs directly or use bookmarks.

Pro Tips:

• Consider using a **browser extension** like uBlock Origin to block trackers and ads

• Use **private/incognito mode** when searching for sensitive topics (but note: this only prevents local history; your ISP and websites can still see your activity)

• Be wary of **URL shorteners** (bit.ly, tinyurl.com) as they can hide the real destination

Phone & Messaging Safety (Score: ___ / 5)

■ I **don't answer calls from unknown numbers** (I let them go to voicemail)

Scam calls are at an all-time high. In 2023, UK consumers received an estimated 4.6 billion scam calls. If it's important, they'll leave a message.

■ I know that **text messages can be spoofed** to look like they're from trusted contacts

Caller ID and sender names can be faked. If you receive an unexpected text asking for personal information or money, verify by calling the person directly.

■ I use **end-to-end encrypted messaging** (WhatsApp, Signal, iMessage) for private conversations

End-to-end encryption means only you and the recipient can read messages. Without it, the messaging company (and potentially hackers) can read your messages.

■ I **don't send sensitive information** (passwords, photos, financial details) via unencrypted channels

Standard SMS texts and some messaging apps are not encrypted. Anything sent can potentially be intercepted or accessed by the service provider.

■ I have **disappearing messages enabled** for sensitive conversations

Apps like WhatsApp and Signal offer disappearing messages that auto-delete after a set time. This reduces the risk if someone gains access to your phone.

Pro Tips:

- Set up **voicemail with a generic message** that doesn't confirm your name or identity
- Be cautious of "one-ring" scams: calls that ring once to get you to call back an expensive premium-rate number
- Remember: **screenshots exist**. Anything you send can be captured, even on Snapchat

Your Privacy Score

Add up your scores from each section:

Section	Max	Your Score
Password Safety	8	___ / 8
Social Media Privacy	8	___ / 8
Personal Information	7	___ / 7
Device & App Settings	8	___ / 8
AI & Chatbot Privacy	6	___ / 6
Browsing & Internet Habits	6	___ / 6
Phone & Messaging Safety	5	___ / 5
TOTAL	**48**	**___ / 48**

Privacy Champion (40 to 48 points)

Excellent! You have strong privacy habits. Keep it up and help others learn too!

Privacy Pro (30 to 39 points)

Good job! You're doing well but there are areas where you can strengthen your defences.

Getting There (18 to 29 points)

You have some good habits but also some significant gaps. Review the sections where you scored lowest and take action today.

At Risk (0 to 17 points)

Your digital privacy needs urgent attention. Work through this worksheet with a parent or guardian and start making changes immediately. Focus on the easiest wins first: setting accounts to private, enabling 2FA, and reviewing app permissions.

The Value of Your Data: Key Facts

Your data is worth money

Tech companies earn an average of **£150 to £250 per user per year** from advertising based on personal data. Google's ad revenue alone was $237 billion in 2023. That's almost entirely funded by user data.

Data brokers sell your information

Companies called **data brokers** collect and sell personal information. The data broker industry is worth over $250 billion globally. They compile profiles containing hundreds of data points about individuals, including estimated income, health conditions, and political views.

Your digital footprint is permanent

Every website visit, search query, social media post, and online purchase contributes to your **digital footprint**. The average person has a digital footprint of **over 70,000 data points**. This data can persist for decades and may affect future opportunities.

Children's data is especially valuable

Children's data is particularly prized because it represents a "full lifetime" of potential marketing. In the UK, the Children's Code (Age Appropriate Design Code) provides legal protections, but many apps still collect more data than necessary.

AI amplifies privacy risks

AI systems can combine scattered bits of data to create surprisingly detailed profiles. A 2023 study showed that AI could correctly infer a person's home address from just 5 seemingly anonymous social media posts.

Your Privacy Rights (UK Law)

Under the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**, you have specific legal rights regarding your personal data:

- **Right to be Informed:** Organisations must tell you what data they collect and why, in clear language
- **Right of Access:** You can request a copy of all personal data an organisation holds about you (Subject Access Request)
- **Right to Rectification:** You can ask for incorrect personal data to be corrected
- **Right to Erasure:** You can ask for your personal data to be deleted ("right to be forgotten")
- **Right to Restrict Processing:** You can ask organisations to limit how they use your data
- **Right to Data Portability:** You can request your data in a format that lets you move it to another service
- **Right to Object:** You can object to your data being used for direct marketing

For children under 13: The ICO's Children's Code requires services to provide high privacy settings by default, not use nudge techniques to weaken privacy, and minimise data collection. If a service violates these rules, you can report it to the **Information Commissioner's Office (ICO)** at ico.org.uk.

My Privacy Improvement Plan

Based on your checkup, write down the **most important changes** you will make. Start with the easiest wins: small changes that make a big difference.

Action 1:

What I will do: _____

Which section does this relate to? _____

I will complete this by: _____

Action 2:

What I will do: _____

Which section does this relate to? _____

I will complete this by: _____

Action 3:

What I will do: _____

Which section does this relate to? _____

I will complete this by: _____

Action 4:

What I will do: _____

Which section does this relate to? _____

I will complete this by: _____

Action 5:

What I will do: _____

Which section does this relate to? _____

I will complete this by: _____

My Privacy Commitment

I commit to protecting my digital privacy and reviewing my privacy settings regularly. I understand that my personal data is valuable and that I have the right to control how it is collected and used.

Signed: _____ Date: _____

Parent/Guardian Signature: _____ Date: _____