Course materials for the teacher

Getting Started Safely Online

10 lessons · approx. 90 minutes of teaching · 21 interactive tasks · As of: 23/11/2026

Phone, class chat, first accounts of your own: how to be smart and safe online from day one, without anyone spoiling the fun.

How the course works

You lead the course at the board and decide yourself when to cover which lesson. The course does not expire. The class does not sign up: no names, no account, no signing in at the start of the lesson. You unlock interactive tasks one by one: a QR code appears on the board for each, the class answers on their phones, and “Reveal” shows the correct answer on the board and on every phone at the same time. The answer key to all quiz questions is in your cockpit; this open PDF deliberately leaves it out so it does not reach the class in advance. At the end you close the course. Nobody in the class registers; there are no names, accounts or e-mail addresses and therefore no individual certificates. This course has no phishing training, which is only part of the course “Digital self-defence”.

What you need: a projector or display with internet access, and the class with smartphones. Anyone without a phone joins in with their neighbour.

Link to the Baden-Württemberg curriculum

Grades 5 and 6 (about 10 to 12 years old) · Scope: two double lessons or four single lessons; lessons can be used individually · As of 03.10.2026

The introduction to the new subject Informatik und Medienbildung (Computer Science and Media Education): follows the reading guide for grades 5 and 6 in the areas of digitality and participation, information and data, and communication and security. Algorithms and digital working stay with subject teaching. Fields of action of the guiding perspective “Living and learning in a digital world”: Acting responsibly and protecting, Communicating, cooperating and acting digitally, Gathering, understanding and evaluating information, Analysing media and the media society.

Area	Competence (reading guide for computer science and media education 2026/27 or 2016 curriculum)

Digitality and participation	Rules for media use at school; describe and reflect on your own media use; identify advertising and explain how it is chosen; terms and conditions of apps; situations where data is collected and the interests of those involved Lessons: Your Day with Your Phone, Advertising, Agree?, Who Do You Tell What?
Information and data	Check information against criteria; criteria for trustworthiness; basic workings of an index-based search Lessons: Is That True?
Communication and security	Communication in the digital space (class chat, rules, consequences); hurtful behaviour, sources of help and ways to report; protecting your own access; storage locations and the path of a message; the right to your own image Lessons: The Class Chat, Strangers Online, Your Lock, Where Is My Photo Stored?
Basic course in media education, grade 5 (becomes part of IuM)	3.1.3 Communication and cooperation (rules online, private data, cyberbullying), 3.1.4 Media society, 3.1.1 Information and knowledge

This mapping is the provider's professional assessment, not an official approval. For grades 8 to 10, the 2016 curriculum applies until the computer science and media education curriculum takes effect (2027/28).

Overview of the lessons

Lesson		Interactive tasks
1.	**Your Day with Your Phone** Grade 5/6 · Digitality and participation How much, what for and why: taking an honest look at your own media use, and what school rules have to do with it.	Word cloud, Quiz
2.	**Advertising: Why the Game Is Free** Grade 5/6 · Digitality and participation Spotting ads in apps and videos, seeing through in-app purchases and understanding why you see exactly these ads.	Quiz, Word cloud
3.	**Agree? What You Sign When You Create an Account** Grade 5/6 · Digitality and participation Terms of use, age limits and permissions: what's behind the "Accept" button and what to check before you tap.	Game: berechtigungen, Quiz
4.	**Who Do You Tell What? Your Data Online** Grade 5/6 · Digitality and participation What data is created when you use apps and games, who is interested in it and why you decide for yourself what you give away.	Game: datenschutz, Quiz

5.	**Is That True? Checking Information** Grade 5/6 · Information and data Where does it come from, who says so, could it even be true? Three questions before believing and forwarding, and how a search engine decides what goes at the top.	Game: faktencheck, Quiz
6.	**The Class Chat** Grade 5/6 · Communication and security Rules that are different in the chat than in the schoolyard, what a joke can turn into, and how you can calm down an argument in the chat.	Word cloud, Quiz
7.	**Strangers Online: Who's Messaging You?** Grade 5/6 · Communication and security Why strangers are nice online, which messages are a warning sign, and where you can get help without getting into trouble.	Quiz
8.	**Your Lock: Password and Screen Lock** Grade 5/6 · Communication and security Why your access is worth protecting, what a good password you can remember looks like, and why you never share it, not even with your best friend.	Game: passwort-knacker, Quiz
9.	**Where Is My Photo Stored?** Grade 5/6 · Communication and security Device, server, cloud: where your stuff really is, which route a message takes through the internet, and why a photo of other people needs their permission.	Quiz, Word cloud
10.	**Summary: Your Starter Toolkit** Supplement · Summary Everything important at a glance, a final quiz and the rules you take away as a class.	Quiz, Quiz, Quiz, Word cloud

The following pages contain each lesson in full, with all quiz questions and answer options. You will find the marked solutions only in your Cockpit.

1. Your Day with Your Phone

How much, what for and why: taking an honest look at your own media use, and what school rules have to do with it.

Let's be honest

When did you first look at your phone today? And when was the last time? Most people underestimate it. Your phone isn't evil, but it is **built to keep you hooked**: notifications, autoplay, "just one more video".

Word cloud

What do you use your phone for most? One word is enough.

What's good for you and what isn't

There's no "right" amount for everyone. But there are signs that it's getting too much:

- You get **irritable** when you're supposed to put your phone away
- Homework takes **twice as long** because something keeps popping up
- You **sleep worse** because your phone is next to your bed
- There are **arguments** at home or with friends because of your phone

> **Important**
>
> You decide, not the app. If you notice that the app is deciding, you've already taken the most important step: paying attention.

Why school has rules

Phones off in class, no photos in the schoolyard, nothing posted from the classroom: these aren't there to annoy you. They protect **everyone** in the room, including you. If you're distracted in class, you miss things. If someone photographs you secretly, you can't defend yourself.



Quiz question

How can you tell that your phone is taking up too much space?

Answer options
I get irritable when I'm supposed to put it away
I sleep worse because it's next to my bed
I use it to meet up with friends
I check when the bus is coming

Tip

Three things that help right away: turn off notifications for games and social media. Phone out of your bedroom at night. One fixed phone-free hour a day, for example during meals.

2. Advertising: Why the Game Is Free

Spotting ads in apps and videos, seeing through in-app purchases and understanding why you see exactly these ads.

Nothing is free

A game costs nothing, a video costs nothing, the app costs nothing. So how do they make money? Almost always in two ways:

1. **Advertising.** Every ad you see earns the app money. The longer you stay, the more.
2. **In-app purchases.** At first everything is free. Then comes the chest, the skin, the extra life, "only €2.99". Lots of small amounts add up to a lot of money.

> **Important**
>
> If you don't pay with money, you pay with your **time** and your **attention**. For the companies, both are worth hard cash.

Spotting ads

Ads like to hide. Look out for:

- **"Ad"**, **"Sponsored"**, **"Advertisement"**, often small and grey
- Influencer videos where a product is "just happening" to be in the picture all the time
- Rewards in a game if you watch an ad video
- Competitions that only want your data

Quiz question

Which of these is advertising?

Answer options
A video where an influencer shows a drink and says "link in bio"
A small grey "Sponsored" above a post

"Watch this video and get 50 coins"
A message from your teacher in the school messenger

Why do you see exactly these ads?

The app remembers what you watch, for how long, and what you tap on. From that it builds a picture of you: "Likes football, watches Minecraft, 11 years old." And then it shows you exactly the ads that fit. This is called **personalised advertising**. That's why your friend sees different ads than you do.

Word cloud

Where did you last notice an ad? One word.

Tip

In-app purchases can be blocked on your phone or protected with a password. Ask at home whether that's set up. It protects you from "bought it by accident".

3. Agree? What You Sign When You Create an Account

Terms of use, age limits and permissions: what's behind the "Accept" button and what to check before you tap.

The button everyone presses

"I have read the terms of use and agree." Be honest: have you ever read them? Hardly anyone does. But with that tap you're entering into a **contract**. That's why it's worth knowing roughly what's in it.

Three things that are almost always in there

1. **Minimum age.** Many services are only for 13 and up, some 16 and up, some 18 and up. That's not a joke: it's about which data from children may be stored and which content is suitable. If you cheat on your age, you lose that protection.
2. **What happens to your data.** Which data is collected, how long it's kept, whether it goes to advertising companies.
3. **What you allow the app to do.** For example: the app may reuse everything you upload.

> **Important**
>
> Agreeing is okay if you know **who** you're allowing to do **what**. It's not okay to tap blindly just because the button is such a nice green.

Permissions: what does the app want from your phone?

After installation, an app often asks: "May I access your contacts? Your location? Your microphone?" Think about it for a moment: **Does the app need that to do its job?**

- A map app needs your location. A torch app doesn't.
- A messenger may need the camera. A game doesn't need your address book.

Learning game



The class rates app permissions on their phones: what does the app really need? Then go through the answers together.

Quiz question

Why do apps have a minimum age?

Answer options
Because children's data is specially protected
Because some content isn't suitable for every age
Because otherwise the app gets too slow
So that adults aren't disturbed

Tip

Before you create an account: check the age limit, tell someone at home, and only grant permissions if the app needs them for its job. You can take them away again in the settings at any time.

4. Who Do You Tell What? Your Data Online

What data is created when you use apps and games, who is interested in it and why you decide for yourself what you give away.

Data is created everywhere

You don't have to type anything for data about you to be created. Just using your phone is enough:

- **Location**: where you are, when you were where
- **Contacts**: who you message, how often
- **Usage**: which videos you watch, for how long, what you skip
- **Device**: which phone, which language, what time

On top of that comes what you post **yourself**: photos, your name, your school, your hobby.

Learning game

Tap the spots in a made-up person's profile that a stranger could use. Then discuss on the board what the class missed.

Who wants to know?

- **Advertising companies**: to show you matching ads (see the last lesson)
- **The app itself**: to keep you there longer and learn more about you
- **Strangers**: anyone who knows where you go to school and when you have training can find you
- **Scammers**: the more they know about you, the more genuine their messages sound

Important

Once something is online, you can hardly get it back. A screenshot is enough. So ask yourself first: **Would I tell this to a stranger on the street?**



You decide

This is called **informational self-determination**: a long phrase for a simple sentence. **Your data belongs to you.** You get to decide what you share, with whom and for how long. Nobody can force you to make your profile public or share your location, not even your friends.

Quiz question

Which details don't belong in a public profile?

Answer options
The name of your school
Your address or where you live, including the street
When you always walk home alone
Your favourite game

Tip

Set your profile to **private**, share your location only when you really need to, and with every photo take a quick look at what's in the background: street sign, school building, name badge.

5. Is That True? Checking Information

Where does it come from, who says so, could it even be true? Three questions before believing and forwarding, and how a search engine decides what goes at the top.

Not everything that looks good is true

Online, **anyone** can write anything. A slick picture, lots of likes, a logo: none of it proves that it's true. That's why there are three questions you ask before you believe something and before you forward it.

The three questions

1. **Where does it come from?** Is there a source? A website, a name, a date? Or just "a friend said"?
2. **Who is saying it and why?** Does the person want to inform, sell, get attention or start an argument?
3. **Could it even be true?** If it sounds too good, too awful or too crazy, it's often made up.

> **Important**
>
> If you can't answer one of the three questions: **don't forward it**. Better to share one thing too few than to spread nonsense once.

Learning game

Five headlines, real or made up? The class votes on their phones, then the board shows the explanation.

How a search engine works

A search engine doesn't "know" anything. It has collected billions of pages in advance and stored them in a huge **index**, like the index at the back of a book. When you type something in, it looks in the index to see which pages contain the word and sorts them: by popularity, by how recent they are, by what other people clicked on, and sometimes

by paid advertising.

That means: **What's at the top isn't automatically right.** At the top is whatever the machine thinks fits, or what someone has paid for.

Quiz question

Why is a result right at the top of the search engine?

Answer options
Because lots of people click on it or link to it
Because someone paid for it (ad)
Because the search engine has checked that it's true
Because it's always the newest one

Tip

Search for the same thing using two different words or on two different sites. If the answers match, that's a good sign. If they contradict each other, ask someone who knows about it.

6. The Class Chat

Rules that are different in the chat than in the schoolyard, what a joke can turn into, and how you can calm down an argument in the chat.

Why the chat is different from the schoolyard

In the schoolyard you see other people's faces. You notice whether a remark goes down well or hurts. In the chat that's missing: **no face, no voice, no pause.** Instead, everyone reads along, everything stays saved, and a screenshot takes two seconds.

That's why things happen faster in the chat that nobody wanted: a joke turns into an insult, a question gets ignored, a picture gets forwarded.

Word cloud

What annoys you most in the class chat? One word.

Rules that work

- **Quiet at night.** No messages after a fixed time, however important.
- **No pictures of others** without asking. Ever.
- **Nothing you wouldn't say out loud in front of the class.**
- **Not everyone has to reply.** Thirty "ok"s are thirty interruptions.
- **Don't fight it out in the chat.** In the chat everything escalates, face to face it doesn't.

> **Important**
>
> Write in a way you'd still be fine with if your grandma or your class teacher read it. Because both can happen.

When things have already gone wrong

Someone gets insulted, an embarrassing picture goes round, someone gets bullied out of the group. Then:

1. **Don't join in.** Not even a laughing emoji. Laughing along is joining in.
2. **Screenshot as evidence**, not to forward.
3. **Say that it's not okay**, ideally directly and calmly.
4. **Get help**: parents, a teacher, a trusted teacher or school counsellor. That's not snitching. Snitching is when you want to hurt someone. Getting help is when you want to protect someone.

Quiz question

Someone posts an embarrassing photo of a classmate in the class chat. What do you do?

Answer options
Not forward it and not react to it
Tell the person that it's not okay
Let a teacher or your parents know
Send a laughing emoji, it was only a joke

Tip

Agree on three chat rules as a class that everyone signs. Three are enough. Put them up in the classroom.

7. Strangers Online: Who's Messaging You?

Why strangers are nice online, which messages are a warning sign, and where you can get help without getting into trouble.

Anyone can be anyone

In a game, in an app, in a chat: you see a name and a picture. Both can be **completely made up**. Anyone could be behind "Lena, 12". Most people online are okay. But the few who aren't are exactly the ones who are so careful and so friendly.

Warning signs

A message is a warning sign if someone you don't know from real life

- **praises you a lot** and says you're something special
- asks whether you're **alone** or whether your parents read along
- wants you to switch to **another chat** where nobody reads along
- asks for **photos**, harmless at first, then less harmless
- offers you **gifts**, in-game currency or skins
- says it's **your secret**

> **Important**
>
> **Secrets with strangers are never okay.** Anyone who asks you to hide something from your parents doesn't mean well. No exceptions.

What you do

1. **Don't reply**, don't argue, don't send anything.
2. **Block and report.** Every app has a button for that.
3. **Tell someone.** Parents, a teacher, an adult you trust. You won't get into trouble. You haven't done anything wrong, the other person has.

And if you've already sent something you regret: **Tell someone anyway.** The sooner, the easier it is to stop. Nobody will punish you for it.



Quiz question

Which message from an online acquaintance is a warning sign?

Answer options
"Are your parents around right now? Let's chat somewhere else."
"This stays our secret, okay?"
"I'll give you skins if you send me a photo."
"GG, well played, see you tomorrow."

Tip

Help, even without giving your name: in Germany, the **Nummer gegen Kummer 116 111** (free, anonymous helpline for children and young people). Report online content in Germany: **jugendschutz.net** (the German centre for youth protection online). And always: an adult you trust.

8. Your Lock: Password and Screen Lock

Why your access is worth protecting, what a good password you can remember looks like, and why you never share it, not even with your best friend.

Why bother?

Your phone and your accounts are like your bedroom: your photos, your chats, your games are in there. Without a lock, anyone who finds your phone or guesses your password can get in. Then suddenly "you" are writing rubbish in the class chat, or someone is buying stuff with your gaming account.

The screen lock

The first and easiest thing: a **lock** for your phone. PIN, pattern, fingerprint or face. Without a lock, nothing else matters. And: **1234** or your date of birth aren't a lock, anyone can guess them.

A good password you can remember

Long beats complicated. The easiest trick: **four words that have nothing to do with each other**, for example `CatBreadRainGuitar`. That's easy to remember and very hard for a computer to crack. Numbers or symbols in between make it even stronger.

Bad ones are: your name, your pet, your favourite team, `password`, `123456` and anything that's on your profile.

Learning game

The class types in sample passwords and sees how long a computer would need to crack them. Only the pattern is transmitted, never the password; it says so on the phones too.

Important

One password, one account. If you use the same one everywhere, one leak means you lose everything at once. And: you **don't share** passwords, not even

with your best friend. Friendships change, passwords stay.

Quiz question

Which password is best?

Answer options
Max2014
password123
CloudPlateLampFrog
111111

Tip

Ask at home whether you use a **password manager**. It remembers all your passwords, you only need to remember one. And wherever possible, turn on **second confirmation** (a code sent to your phone): then a stolen password alone is useless.

9. Where Is My Photo Stored?

Device, server, cloud: where your stuff really is, which route a message takes through the internet, and why a photo of other people needs their permission.

Three places

When you take a photo, it's first stored **on your device**. If you send it to a chat, it's also stored **on a server** belonging to the provider, a big computer in a data centre. If you switch on backup, it's also in the **cloud**: another server, except you can use it like a folder.

Place	Advantage	Disadvantage
Your device	Only you have it	Phone gone, photo gone
The chat's server	Your friends get it	The provider has a copy, even if you delete it
Cloud	Available everywhere, backup	Stored by a company, often in another country

> **Important**
>
> "Deleted" on your phone doesn't mean deleted on the server. What you send isn't only yours any more.

The route of a message

The internet isn't a single wire but a **network of many nodes**: your phone, the Wi-Fi router, the provider, servers somewhere in the world, your friend's router, her phone. Your message jumps from node to node, and if one fails, it takes a different route. That's what makes the network so robust. And it means: on the way, your message passes lots of other people's computers. That's why **encryption** is important; you'll learn more about it in later years.

Your phone is the **client** (the one that asks), the server is the one that answers. Every app and every website works like this.

Quiz question

You delete a photo from the chat on your phone. What's true?

Answer options
It may still be on the provider's server
Anyone who has already received it still has it
It's gone everywhere
The provider is notified immediately and deletes it

Photos of other people

Everyone has a **right to their own image** (in Germany this is called *Recht am eigenen Bild*). That means: you may only pass on or post a photo in which someone can be recognised if that person **agrees**. With classmates, that means: ask first. If they say no: don't post it. Not even "just in the class chat".

Word cloud

Who would you have to ask before posting your last group photo? One word: everyone, nobody, teacher, ...

> **Tip**
>
> Three seconds before sharing a photo: Who's in it? Have I asked? What can be seen in the background?

10. Summary: Your Starter Toolkit

Everything important at a glance, a final quiz and the rules you take away as a class.

What you can do now

You decide, not the app. Notifications off, phone out of the room at night, one phone-free hour.

Nothing is free. Spot ads, block in-app purchases, know why you see exactly these ads.

Agree with your brain switched on. Take minimum ages seriously, grant permissions only if the app needs them.

Your data belongs to you. Private profile, no school name, no address, no daily routine.

Check first, then believe. Where from? Who? Could it be true? What's at the top of the search isn't automatically right.

In the chat like in the schoolyard, only more careful. No pictures without asking, nothing you wouldn't say out loud, no fights in the chat.

Strangers stay strangers. Secrets with strangers are never okay. Block, report, tell someone. In Germany: Nummer gegen Kummer 116 111.

Your lock. Screen lock, four words as a password, never share it.

Deleted isn't deleted. What you send is stored on servers. Photos of others only with permission.

> **Important**
>
> You don't have to do everything perfectly. If you know these rules, you're already much safer than most adults.

Final quiz

Quiz question

What do you do if an online acquaintance says: "This stays our secret"?

Answer options
Don't reply, block, tell an adult
Play along, it's only a game
Wait and see what else he writes
Send a photo so he leaves you alone

Quiz question

Which three questions do you ask before forwarding a message?

Answer options
Where does it come from?
Who is saying it and why?
Could it even be true?
How many likes does it have?

Quiz question

What's part of good protection for your phone?

Answer options
A screen lock that isn't 1234
A long password made of several words
Not sharing your password with friends
The same password everywhere so you don't forget it

Word cloud

Which rule are you taking away from this course? One word.

> **Tip**
>
> Teacher: agree on the three chat rules from the class chat lesson together now and put them up. That's what will last longest from this course.