

DIGITAL COMPASS

DRONE Handbook for Parents



Funded by
the European Union



This handbook was written in 2025 as part of the EU-funded DRONE project. It was edited and prepared for digital publication in 2026. DeepL Translator Pro was used for the first version of the translations, no other AI tool was used in creating the contents of the handbook and the other handbooks in this 3-book series.

The book was designed and typeset for PDF distribution using Adobe Creative Cloud, with attention to screen readability and long-form digital reading.

First digital (PDF) edition published in 2026.

© 2026 Eszter Salamon, Aristidis Protopsaltis

Editor: Judit Horgas

Design: Emanuele Bertolani



CC BY-NC-SA 4.0

Creative Commons Attribution: Non-commercial-Share Alike 4.0 International

This license requires that re-users give credit to the creator. It allows re-users to distribute, remix, adapt, and build upon the material in any medium or format, for non-commercial purposes only.

👤 BY: Credit must be given to you, the creator.

🚫 NC: Only non-commercial use of your work is permitted.

🔄 SA: If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

Non-commercial means not primarily intended for or directed towards commercial advantage or monetary compensation.

You are free to share and adapt this material for non-commercial purposes, provided appropriate credit is given, changes are indicated, and any derivative works are distributed under the same license.

A copy of the license is available at:

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

ISBN: [ISBN, if applicable]

File format: PDF

Published by Parents International, a member of the DRONE Project consortium

The DRONE Handbooks are designed for use by parents or carers, teachers, school heads, and trainers. Their primary purpose is to foster Digital Literacy and counter disinformation. The handbooks are flexible and can be adapted to suit various contexts and individual needs. For some users, they serve as an accessible introduction to the fundamentals of Digital Literacy and Disinformation, presenting essential concepts and practices in straightforward language. For others, the handbooks offer practical guidance on integrating Digital Literacy and Disinformation topics into learning activities for young people, whether in formal classrooms or non-formal educational environments. Additionally, the handbooks are valuable resources for those planning Digital Literacy and Disinformation Education programmes or courses for other educators or trainers. In schools and similar formal educational settings, it is recommended to coordinate with the institution's data protection officers when using these handbooks.

TABLE OF CONTENTS

Chapter 1 - Information Literacy.....	19
Chapter 2 - Disinformation, Misinformation and Fake News.....	31
Chapter 3 - Resilience Building.....	41
Chapter 4 - Problem-solving.....	53
Chapter 5 - Critical Thinking.....	63
Chapter 6 - Bullying and Cyberbullying.....	73
Chapter 7 - Cybersecurity.....	87
Chapter 8 - Building Alliances.....	97
Checklists.....	105
Toolbox Guides.....	109
Annexes.....	127

This handbook is your practical guide to supporting your child in today's digital world. It was created to help you build confidence, recognise risks, and strengthen the habits and conversations that help children stay safe, informed, and emotionally resilient online.

You do not need to be a technology expert. This handbook is designed in clear, accessible language and grounded in real-life situations families face every day.

How to get the most out of it

1. Begin with yourself

Your digital habits influence your child's. Use the reflection questions and checklists to understand your own strengths and areas for growth.

2. Dip in when needed

E.g. if your child is facing online challenges today, start with the bullying or resilience chapters; if you're confused about a viral claim they've brought home, go straight to misinformation and critical thinking.

Each chapter stands alone. Start wherever your current concern lies:

- If your child is struggling with a viral claim: go to **Misinformation** and to **Critical Thinking**
- If they're facing online conflict: read **Bullying & Cyberbullying**
- If they are overwhelmed or anxious: explore **Resilience**

3. Use the activities together

Many exercises and conversation prompts are designed for shared learning. Explore them with your child so you can learn side-by-side – not as the “expert,” but as a co-learner.

4. Take a practical approach

Try the checklists, troubleshooters, and “when things go wrong” steps. They are meant for real homes with real pressures and limited time.

5. Reach out and connect

Use what you learn to start conversations with teachers or other parents. Stronger alliances help protect children far more effectively than isolated efforts.

6. Return to it often

Technology changes quickly, and so do children's digital habits. Revisit the handbook as new issues or questions arise.

This handbook is a companion for daily family life. It isn't about perfection. It's about support, curiosity, communication, and resilience. Use it to build a safer, more balanced digital environment at home – one that helps your child grow into a confident, critical, and emotionally secure digital citizen.

If You Want to Go Deeper

Explore the matching modules from the DRONE online course or look for in-person training opportunities. These complement the handbook with more examples and guided learning.

Access the DRONE website here: <https://mydroneproject.eu/>

HOW TO USE THIS HANDBOOK

The DRONE resources – a collection of training modules and three handbooks – were designed as a comprehensive, interconnected collection of tools that support digital literacy, resilience, responsible online behaviour, and the prevention of digital harm across the whole school community. Each resource plays a different role, but together they provide a 360-degree support system reaching students, families, teachers, and leadership teams. The purpose of this collection of resources is simple but powerful: to build a digitally confident, critically aware, and emotionally resilient learning community.

You may use the resources individually or as a cohesive system – whichever best fits your needs. Every resource – from full chapters to short guides – is a step toward that goal.

What is included?

1. Three Full Handbooks

Each handbook is tailored to a different audience:

- DRONE Handbook for Parents
- DRONE Handbook for Teachers
- DRONE Handbook for School Leaders

Although the structure is shared, each book includes audience-specific case studies, strategies, and responsibilities. Parents focus on home practices; teachers focus on pedagogy; school leaders focus on policy and whole-school systems.

2. Training modules for teachers, school leaders, and parents

Each training module is available in three different formats. An online version is developed for independent online learning, and downloadable resources are available for organising an in-person or a synchronous online training session.

Each of the three target groups has a choice of training modules that can be used independently from other modules on the following topics:

- Information literacy
- Disinformation, misinformation, and fake news
- Resilience building
- Problem-solving
- Critical thinking
- Bullying and cyberbullying
- Cybersecurity
- Building alliances

How the Pieces Fit Together

Parents

- Begin with your Parent Handbook for full understanding.
- Use the Quick Cybersecurity Guide, Bullying Toolkit, and Conversation Guide for everyday support.
- Explore the reading lists to build long-term digital awareness at home.
- If you want to dig deeper and you haven't done training on a topic before, check the relevant training module to learn more.
- If you feel that teachers need to know more, recommend the teacher resources to them.

Teachers

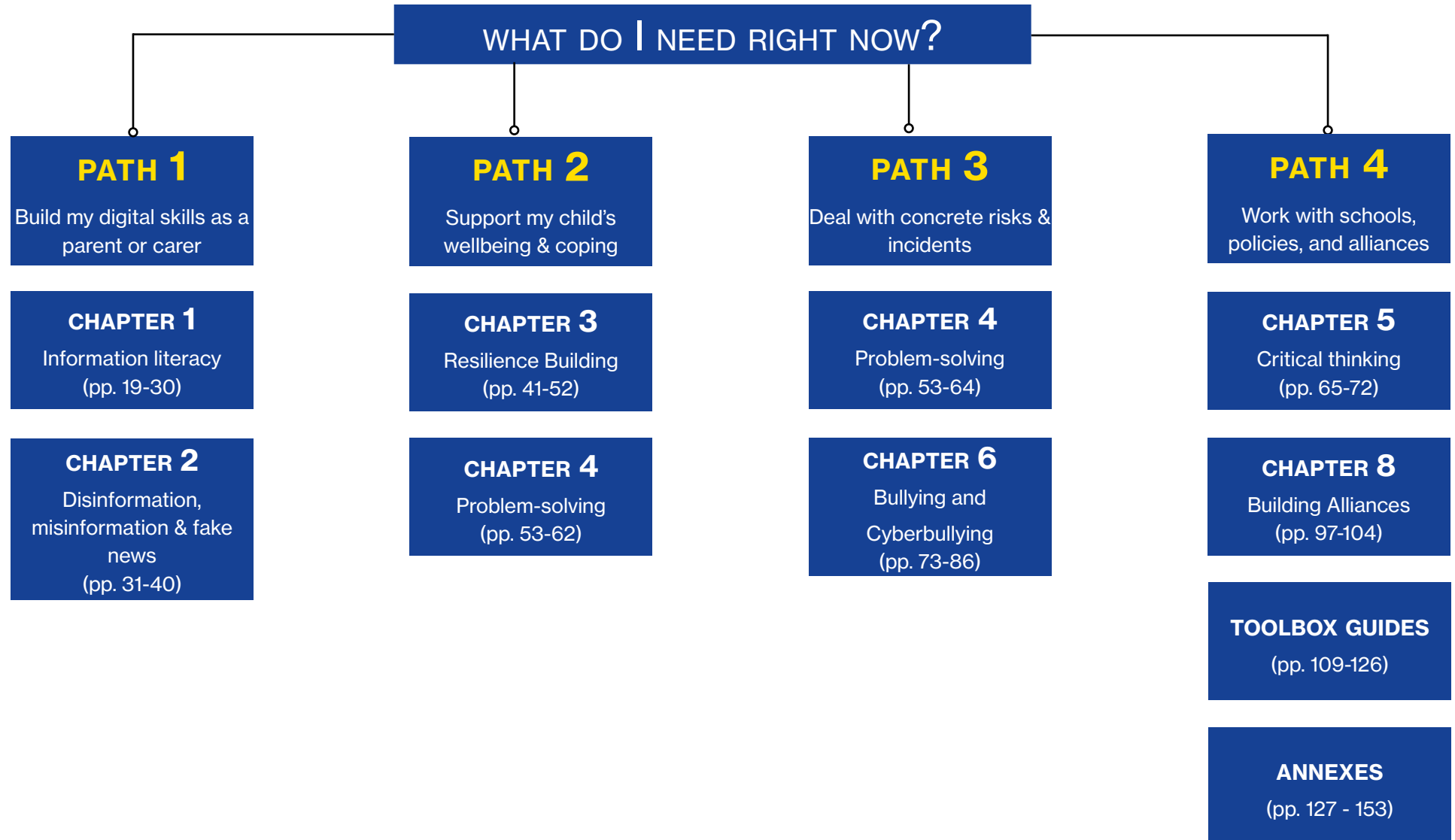
- Start with the Teacher Handbook to build your own digital competence.
- Keep the Teacher Quick Reference Guide in your classroom or staffroom.
- Use student-facing tools (Digital Survival Guide, etc.) in lessons or tutor sessions.
- Refer to case studies and toolkits during incidents involving misinformation, bullying, or online conflict.
- If you want to dig deeper and you haven't done training on a topic before, check the relevant training module to learn more.
- If you think parents of your students need more support, recommend the parent resources to them.

School Leaders

- Use the School Leader Handbook to shape policy, risk assessment, and digital culture.
- Share the Quick Guides with staff and parents to build consistent understanding.
- Use the toolkits to support staff training and community engagement.
- Refer to reading lists, research summaries, and the teacher resources when designing school-wide CPD.
- If you want to dig deeper and you haven't done training on a topic before, check the relevant training module to learn more.
- If you think parents of your students need more support, recommend the parent resources to them.

WHERE TO FIND WHAT IN THIS HANDBOOK

Find your path through this handbook (click to access the desired section)



INTRODUCTION: OVERVIEW OF DIGITAL LITERACY AND DISINFORMATION

Why parents' and carers' digital literacy matters

Parents' and carers' digital literacy plays a crucial role in shaping how children understand and navigate the digital world. The ability to effectively guide, model, and discuss online behaviours depends largely on one's own skills and awareness. By developing digital competence, parents can take a proactive approach that not only reduces potential risks of harm but also strengthens trust and open communication with their child.

Why digital literacy matters for children and adolescents

Digital literacy is essential for children and adolescents because their well-being, learning, and development are now deeply intertwined with online experiences. Without the skills to navigate the digital world critically and safely, they become vulnerable to believing false health claims, experiencing cyberbullying, falling victim to scams, or being overexposed to harmful online communities.

The role of parents and carers (from DRONE research)

The DRONE project emphasises three roles for parents and carers:

1. **Mentor** – learn together and encourage critical thinking
2. **Model** – demonstrate safe and thoughtful online behaviour
3. **Protector** – put safeguards in place and intervene when needed

Digital literacy is more than a set of technical skills. At its core, it is the ability to use digital tools and platforms effectively, responsibly, and critically. This includes everyday tasks such as searching for information, communicating online, or using apps, but it also extends to deeper competences: evaluating the reliability of information, recognising manipulative content, protecting one's privacy, and engaging in respectful online behaviour.

In today's digital age, information travels faster than ever before. A single post, video, or meme can reach millions of people within hours, regardless of whether it is true or false. This reality makes digital literacy not just helpful but essential. Being digitally literate means more than operating a smartphone or browsing the internet; it means developing a sharp sense of judgment about what to believe, share, or ignore.

Alongside the opportunities of the digital world, we also face real challenges. Disinformation, misinformation, and fake news affect both adults and children. These terms are often used interchangeably, but they are not the same:

- **Misinformation** is false or inaccurate information.. For example, a relative might share a health “tip” on social media, believing it to be helpful, even though it is not based on evidence.
- **Disinformation** is false information which is deliberately intended to mislead – intentionally misstating the facts. It is deliberate misinformation. This includes conspiracy theories, manipulated videos, or propaganda campaigns.
- **Fake news** is a popular but sometimes misleading label, often referring to fabricated stories presented as legitimate news articles.

All of these can mislead, confuse, or manipulate, sometimes with serious consequences. For young people, who are still learning to evaluate the world around them, the risks are even greater.

As a parent or carer, your own digital literacy plays a vital role. Children learn not only from what we tell them but from what they see us do. When you pause before sharing an article, ask questions about online sources, or model respectful online communication, you are teaching your child far more than rules - you are giving them lifelong skills to navigate an increasingly complex digital landscape.

Why Digital Literacy Matters for Parents and Carers

Parents and carers are often the first line of defence in helping children navigate online spaces. Your knowledge, attitudes, and habits directly influence how your child interprets the digital world.

Strengthening your own digital literacy means you are better equipped to:

- Recognise risks and opportunities: whether it's understanding how gaming platforms collect data, recognising scams, or supporting your child to use online resources for learning, your awareness sets the tone for safe and productive use.
- Support resilience and critical skills: children face a mix of positive and negative online experiences. Your guidance can help them build the strength to cope with challenges such as cyberbullying or exposure to harmful content, and the critical skills to spot misinformation.
- Respond constructively when things go wrong: no system is perfect. Mistakes will happen, and children will sometimes stumble into harmful or misleading content. The difference lies in how adults respond – calmly, with empathy, and with practical steps.

Example: A Parent's Influence

Consider two scenarios. In the first, a teenager shares a conspiracy video about health risks. The parent dismisses them harshly, saying, "That's nonsense, don't be stupid." The young person feels embarrassed and retreats, but may continue to believe the video privately.

In the second scenario, the parent says, "That video is interesting – but let's check it together. Who made it? Can we find another source? Why do you think it was made?" This approach validates the child's curiosity while guiding them to think critically. Over time, the second approach builds confidence and trust.

Why Digital Literacy Matters for Children and Adolescents

Children and adolescents are digital natives, but that does not mean they are digitally literate. They are highly skilled at navigating apps, creating content, and engaging in digital communities, yet they may lack the judgment to evaluate what is safe, trustworthy, or ethical.

Digital environments shape almost every aspect of their lives:

- **Education:** Online platforms, digital textbooks, and virtual classrooms are now common parts of schooling.
- **Friendships:** Social media and messaging apps are central to how young people connect and maintain relationships.
- **Leisure:** Games, videos, and streaming platforms are their main sources of entertainment.
- **Identity:** Online spaces increasingly influence how young people see themselves and others.

Without strong digital literacy, children can be vulnerable to:

- Believing false or manipulative information.
- Engaging in unsafe online behaviour, such as oversharing personal data.
- Becoming victims (or perpetrators) of cyberbullying.
- Being targeted by online exploitation or scams.
- Experiencing anxiety, low self-esteem, or other negative effects of digital comparison and pressure.



THE VIRAL CHALLENGE

A group of adolescents encounter a viral online “challenge” encouraging risky behaviour. Some believe it is fun and harmless, others are unsure, but none check where it came from. A digitally literate child would pause and question: Who created this? What could happen if I try it? Is this safe? With parental guidance, children can learn to apply these critical questions instinctively, reducing the chance of harm.

ROLE OF PARENTS AND CARERS: INSIGHTS FROM DRONE RESEARCH

The DRONE project emphasises that parents and carers are not just supervisors of children's online activities. They are mentors, role models, and co-learners. Children do not benefit from surveillance alone; they need open conversations, shared exploration, and emotional support.

According to DRONE findings, effective parental roles include:

- Learning alongside your child: You don't need to be an expert. Admitting, "I don't know, let's find out together," models healthy curiosity and humility.
- Main educators: Students reported that currently they receive little support at school in their digital literacy development, so you need to fill this gap or know who to turn to for help.
- Encouraging open conversations: Make it safe for your child to talk about online experiences – even the negative ones – without fear of punishment.
- Providing emotional and practical support: Help children process feelings about online experiences, whether it's the sting of exclusion from a group chat or the confusion of encountering harmful content.
- Building a safe digital environment at home: Set age-appropriate boundaries, such as screen time limits, device-free dinners, or shared family accounts, but combine rules with guidance and reasoning.

Mentorship Over Monitoring

While many parents rely on monitoring apps or controls, research shows that mentorship is more effective than surveillance alone. Monitoring can sometimes backfire, leading to secrecy and distrust. In contrast, when children see parents modelling critical engagement with media and encouraging dialogue, they internalise those behaviours.

Practical Steps for Parents and Carers

- Check your own habits: Are you modelling the behaviour you want your child to learn? For example, do you fact-check before sharing? Do you maintain respectful tone in online debates?
- Use teachable moments: When misinformation arises in the news or social media, use it as a chance to discuss how to evaluate it.
- Balance supervision with trust: Younger children need closer monitoring, but as they grow, shift towards mentoring and supporting independence.
- Keep conversations ongoing: Rather than a one-off “online safety talk,” make digital life a regular part of family discussions.
- Seek support and resources: You are not alone. Schools, community organisations, and initiatives like DRONE provide tools, workshops, and resources.

DIGITAL LITERACY: PRACTICAL STEPS FOR PARENTS AND CARERS



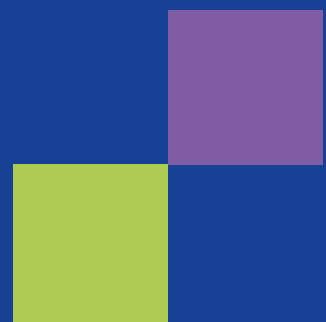


A FAMILY APPROACH

A parent noticed their 11-year-old spending hours watching videos on a platform. Some videos were harmless entertainment, but others promoted extreme views. Instead of banning the platform, the parent watched a few videos with the child and asked, "What do you think of this person's opinion? How do we know if it's true?" Together, they searched for other sources and compared perspectives. Over time, the child began pausing videos to question them, developing healthier habits.

CHAPTER 1

INFORMATION LITERACY



WHAT IS INFORMATION LITERACY?

Information literacy is the ability to find, evaluate, and use information effectively. In simple terms, it is about asking the right questions:

- Who wrote this?
- Why was it published?
- Can I trust it?
- What evidence supports it?

In the digital age, children and adults are exposed to vast amounts of information every day. Some of it is accurate and useful, but much of it is biased, incomplete, misleading, or even deliberately false. Without strong information literacy skills, it is easy to become overwhelmed, misled, or even manipulated.

Being information literate is not about memorising facts. Instead, it's about learning how to approach information critically – weighing its reliability, comparing different sources, and deciding how best to use it. For parents, this skill is especially important because it shapes how you guide your children's understanding of the world.

DEVELOPING YOUR COMPETENCES AS A PARENT OR CARER

As a parent or carer, you are a role model for your child's digital habits. When you show that you check sources, question claims, or admit when you don't know something, you are teaching your child valuable habits that they will carry into adulthood.

Here are some practical ways to strengthen your own information literacy:

1. Practise Fact-Checking News Items

Before sharing an article, video, or meme, take a moment to check:

- Is the source reputable?
- Can the information be verified in at least two other trustworthy places?
- Does the headline match the content of the article, or is it designed to provoke emotion?

Tools like Google Reverse Image Search, Snopes, or Full Fact can help you identify manipulated images or debunk common myths.

2. Use Reputable Sources for Parenting Information

When it comes to health, education, or parenting, misinformation is widespread online. Blogs or social media posts often share “tips” that may be untested or harmful. Instead, use reliable sources such as national health services, education ministries, or well-established child development organisations.

3. Model Healthy Online Behaviours

Children notice how parents behave online. If you pause to question an article or explain why you don't share a particular post, you are showing them how to handle information responsibly.

Example:

Your child sees you reading a headline that claims, “Chocolate cures stress instantly!” Instead of laughing it off or sharing it, you might say, “That sounds nice, but let's see if scientists agree. Let's check a medical site.” This small action demonstrates how to think critically without dismissing curiosity.

SUPPORTING YOUR CHILD'S INFORMATION LITERACY

Children and adolescents are growing up in a world where information overload is the norm. Their ability to distinguish between truth and falsehood often depends on the guidance they receive at home.

Here are strategies you can use:

1. Encourage Curiosity Through Questions

When your child tells you something surprising they found online, respond with curiosity, not judgment. Ask:

- Where did you hear that?
- Do you think the person who wrote it knows a lot about the topic?
- Why do you think they posted it?

This turns conversations into learning opportunities.

2. Teach Simple Evaluation Strategies

Children don't need complex media theory to start. Begin with simple steps:

- Check the date of a post – is it recent or outdated?
- Look for the author's name – do they have expertise?
- Compare it with another source – does the story appear elsewhere?

3. Share Activities Together

Information literacy can be practised as a family. For example:

- Compare headlines from different news outlets about the same event. Discuss how wording changes perception.
- Play a “truth or trick” game where you present short stories (some true, some false) and work together to decide which is which, explaining why.
- Explore fact-checking websites together and see how they explain false claims.



A FAMILY NEWS NIGHT

One family made a weekly routine of looking at three different news websites together. Each person picked a story, and the family compared how each outlet presented it. Over time, the children became more confident in spotting bias and asking critical questions about news they encountered on social media.

WHEN THINGS GO WRONG

Despite your best efforts, children may sometimes believe or share false or harmful information. This is a natural part of learning – just as children make mistakes in maths or spelling, they will also make mistakes in evaluating information. The key is how you respond.

Warning Signs of Poor Information Literacy in Children

- Repeating extreme or false claims without question.
- Sharing harmful or misleading content online.
- Expressing confusion about what is true or trustworthy.
- Showing emotional distress after encountering conflicting information.

How to Respond

1. Stay Calm and Avoid Blame

Reacting with anger or ridicule can make children defensive and less willing to share in the future. Instead, thank them for sharing, even if the content is wrong.

2. Show How to Fact-Check Together

Sit down and explore the claim side by side. Use it as a chance to practise critical thinking rather than a moment for punishment.

3. Encourage Reflection

Ask questions like:

- What made you believe this at first?
- How do you feel now that we've checked it?
- What could we do differently next time?

4. Contact Teachers if Needed

If the issue escalates – for example, if your child is spreading misinformation widely or facing bullying because of false claims – involve teachers. Schools often have resources or lesson plans to support media literacy, and your child may benefit from reinforcement in the classroom.

HOW TO RESPOND TO POOR INFORMATION LITERACY IN CHILDREN

STAY CALM AND
AVOID BLAME ●



● SHOW HOW TO
FACT-CHECK
TOGETHER

ENCOURAGE
REFLECTION ●



● CONTACT TEACHER
IF NEEDED



CASE STUDY 1: THE VIRAL HEALTH CLAIM

A 13-year-old shares a video claiming that drinking a special tea cures all illnesses. The parent notices the child repeating the claim to friends. Instead of dismissing it, the parent asks: "Where do you think that idea came from? Should we check what doctors say?" Together, they search reliable health websites and discover the claim is false. The child feels included in the process and learns to double-check health information.

CASE STUDY 2: POLITICAL MISINFORMATION

A 15-year-old begins sharing extreme political content online, convinced it is factual. The parent recognises the content as biased and misleading but avoids confrontation. Instead, they watch a video together and then ask: "Who do you think benefits from us believing this? Is there another side to the story?" Over time, the young person develops a more balanced perspective, learning that not everything online is neutral.

CASE STUDY 3: CONFUSION IN THE CLASSROOM

An 11-year-old argues with classmates about a story they read online, feeling embarrassed when others correct them. At home, the parent helps the child look up the claim together and shows how to use fact-checking websites. Later, the parent contacts the teacher to suggest a class-wide discussion about evaluating information. The incident becomes a shared learning opportunity instead of a source of shame.

PRACTICAL TOOLS FOR PARENTS

Information Literacy Checklist

- Do I pause before sharing content online?
- Have I checked who created it and why?
- Can I confirm it in at least two other places?
- Am I modelling this process for my child?

Conversation Starters with Children

- That's interesting – where did you hear it?
- Do you think the person who posted it has expertise?
- Can we check another source together?
- Why do you think someone would want us to believe this?

Family Challenge

Once a week, pick one surprising headline and test it together. Score yourselves on how quickly you can decide if it's true or not. Make it fun, not a test.

CONCLUSION

Information literacy is a core life skill in the digital age. For parents and carers, developing your own competences is the first step – you cannot teach what you do not practise. By fact-checking, questioning, and modelling healthy digital behaviours, you create a powerful example for your child.

Supporting your child's information literacy is not about restricting curiosity but about guiding it. Encourage questions, explore information together, and show that being thoughtful is more important than being right on the first try. When things go wrong, approach the situation with calm curiosity and shared problem-solving. Mistakes are opportunities for growth. With your support, your child can develop the resilience and skills to navigate digital worlds safely, responsibly, and with confidence.

Building your competences

- Use fact-checking websites such as [Snopes](https://www.snopes.com/) (<https://www.snopes.com/>), EU vs [Disinfo](https://fullfact.org/) (<https://fullfact.org/>), or [Full Fact](https://euvsdisinfo.eu/) (<https://euvsdisinfo.eu/>)
- Practise comparing the same story across multiple outlets.
- Reflect on your own habits: Do you share content before checking it?

Supporting your child

- Create a family routine of checking headlines together.
- Ask your child to explain where they found information.
- Praise curiosity and reward healthy scepticism.

When things go wrong

If your child consistently struggles to distinguish reliable sources:

- Gently correct misinformation without ridicule.
- Share examples of credible sources in plain language.
- Involve teachers in strengthening research assignments.

Suggested reading:

- “Media and Information Literacy Curriculum for Teachers” (UNESCO). ¹
- “EU Kids Online 2020: Survey results from 19 countries”. ²

1. <https://www.unesco.org/en/articles/media-and-information-literacy-curriculum-teachers>

2. <https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf>

In everyday conversation, the phrase “fake news” is often used as a catch-all for anything untrue or misleading online. But when helping children and adolescents understand the digital world, it is important to distinguish between misinformation, disinformation, and fake news.

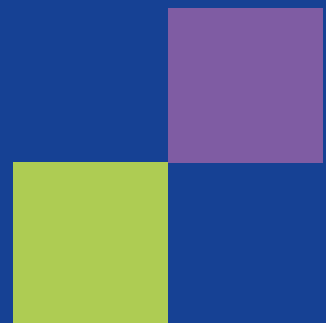
- **Misinformation**: False or inaccurate information shared without the intent to harm. Example: a family member shares a social media post about a “miracle cure” because they genuinely believe it will help others.
- **Disinformation**: false information which is deliberately intended to mislead – intentionally misstating the facts. It is deliberate misinformation.. Example: a fabricated story about an election designed to mislead voters.
- **Fake news**: A popular label for fabricated or manipulated stories that are presented in the format of news articles or reports.

Understanding these distinctions matters because the intent and impact differ. Misinformation may spread accidentally, while disinformation is often carefully planned to manipulate public opinion, earn money through clicks, or create division.

Children are particularly vulnerable because they are still learning to interpret the world. They may not yet understand how algorithms amplify extreme content, or how online creators can profit from views, regardless of accuracy.

CHAPTER 2

DISINFORMATION, MISINFORMATION AND FAKE NEWS



DEVELOPING YOUR OWN SKILLS AS A PARENT OR CARER

Before you can teach your child to spot misleading content, you need to be confident in recognising it yourself. Many adults struggle with this, and that is normal. The good news is that there are practical steps you can take to strengthen your own ability.

1. Learn the Common Signs of Disinformation

Misleading content often has recognisable “red flags”:

- Sensational or shocking headlines designed to grab attention.
- Emotional language that plays on fear, anger, or outrage.
- Lack of credible author or organisation.
- Absence of supporting evidence or references.
- Claims that appear only in one place or are shared only on social media.

2. Practise Before You Preach

Try fact-checking the next surprising story you see online. Use tools such as:

- Snopes (general fact-checking).
- Full Fact (UK) or similar regional services.
- EUvsDisinfo (European disinformation campaigns).
- Google Reverse Image Search (to spot reused or altered photos).

The more you practise, the more automatic the habit will become – and the more natural it will feel to model this process for your child.

3. Reflect on Your Own Biases

We are all more likely to believe information that fits our existing opinions. Being aware of this helps you approach online content with humility and curiosity, which is exactly the attitude you want to pass on to your children.

SUPPORTING YOUR CHILD IN SPOTTING MISLEADING CONTENT

1. Create a Culture of Curiosity

Instead of telling your child “that’s wrong” or “don’t believe everything online,” ask questions that encourage critical thinking:

- Who created this?
- Why do you think it was posted?
- What do other sites say about it?
- How does it make you feel?

This not only develops analytical skills but also strengthens trust – your child sees you as a partner in learning rather than a judge.

2. Teach “Pause Before Share”

Many young people share content instantly without thinking. Encourage the simple rule: Pause. Check. Then share. Even a 30-second pause to reflect or verify can prevent the spread of false information.

3. Use Real-Life Examples

Children learn best through practice. Pick an example of viral misinformation (such as a health myth, a doctored photo, or a misleading meme) and go through it together:

- Compare it with reliable news sources.
- Look up the image to see if it has been used before.
- Discuss what could happen if people believe and act on it.

WHEN THINGS GO WRONG

Sometimes children will fall for misinformation or even share disinformation themselves. This is not a sign of failure – it is a natural learning stage. However, you may have to correct misinformation or disinformation brought home from school, shared by teachers. The goal is not to prevent all mistakes but to help children learn from them safely.

Warning Signs

- Your child repeats extreme or unlikely claims as facts.
- They share misleading content on social media without checking.
- They argue strongly for an idea but cannot explain where it came from.
- They become anxious or fearful after consuming alarming content.

How to Respond

1. Stay Calm

Avoid scolding or mocking. Children who feel shamed may withdraw and continue to believe false claims privately.

2. Investigate Together

Sit down and go through the content step by step. Ask: “Let’s see where this comes from. Can we find another source?” Carefully decide if you also sit down with the teacher if the information seems to come from them.

3. Highlight the Real-World Impact

Explain how misinformation can cause harm – from wasted money on fake products to serious consequences like health risks or prejudice.

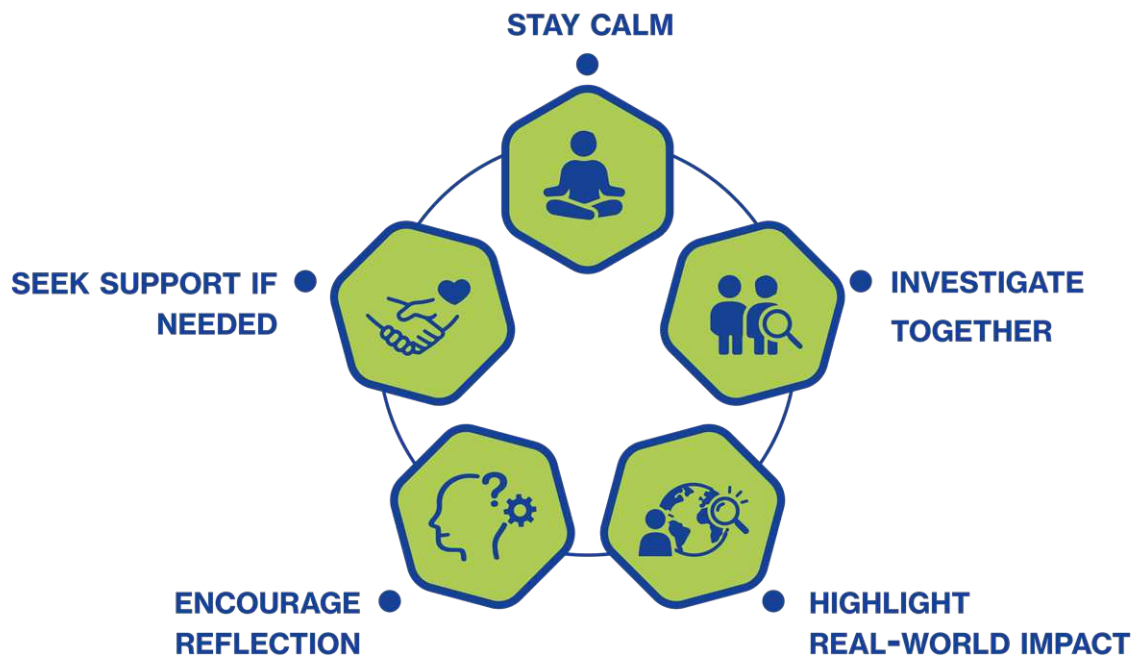
4. Encourage Reflection

Ask: “What made you believe it at first? How could we check next time?” This helps your child develop awareness without fear of being “caught out.”

5. Seek Support If Needed

If your child is deeply involved in extremist or harmful online groups, contact their teacher or school counsellor. Schools can address misinformation within the curriculum and offer guidance.

HOW TO RESPOND TO MISINFORMATION OR DISINFORMATION IN YOUR CHILD





CASE STUDY 1: THE CELEBRITY RUMOUR

A 12-year-old insists that a favourite celebrity has died, after seeing multiple social media posts. The parent resists the urge to dismiss it and instead checks official news websites with the child. They discover the story is false, created as a prank. The parent explains why people spread such rumours – often for attention or clicks. The child learns not to trust viral claims without checking.

CASE STUDY 2: THE FAKE HEALTH TIP

A teenager shares a “natural cure” video with friends, claiming it can replace medical treatment. The parent recognises the danger and calmly sits down with the teen. Together, they search reputable health sites and learn the claim is false and risky. The teen feels respected in the process and becomes more cautious about health content in the future.

CASE STUDY 3: THE POLITICAL MEME

A 15-year-old begins reposting political memes that exaggerate or distort facts. Rather than confronting them, the parent asks: “Who do you think made this? What do they want us to believe?” This sparks a conversation about propaganda and persuasion. The young person begins to recognise the difference between facts, opinions, and manipulative tactics.

PRACTICAL TOOLS FOR PARENTS

Quick Red Flags for Misleading Content

- All caps or sensational headlines.
- Emotional appeals (“This will shock you!”).
- No clear author or organisation.
- Poor grammar or design.
- One-sided argument without sources.
- Urgency to share quickly (“Don’t let this be deleted!”).

Conversation Starters with Children

- Why do you think people make up stories online and try to make others believe they are true?
- What could happen if someone believed this?
- Should we check this in another place?
- What would you do if a friend sent this to you?

Family Fact-Checking Routine

- Once a week, pick a piece of online content together.
- Test it using at least two fact-checking tools.
- Score yourselves on how quickly you can find out if it’s true.
- Celebrate the process, not just the “right answer.”

CONCLUSION

Disinformation, misinformation, and fake news are among the greatest challenges of the digital age. But they are not unbeatable. With the right skills, families can navigate these challenges with confidence.

For parents and carers, the first step is developing your own competences – learning to spot red flags, practising fact-checking, and reflecting on your own online habits. From there, you can guide your child through questioning, curiosity, and shared exploration.

When mistakes happen, they should be treated as teachable moments, not failures. Every false claim debunked together is a step towards stronger critical thinking. Every open conversation builds resilience against manipulation.

The DRONE project reminds us that parents and carers are not passive observers but active mentors in the digital journey. By learning alongside your child, you are preparing them not just to survive but to thrive in a world where truth and lies often compete for attention.

Understanding the differences

- **Misinformation**: Incorrect information shared without harmful intent.
- **Disinformation**: False information created to manipulate or deceive.
- **Fake news**: A subtype, often sensationalised, imitating journalism.

Building your awareness

- Learn the emotional cues: exaggerated headlines, capital letters, urgent calls to action.
- Check if the content is satirical or parody.
- Be aware of algorithmic amplification – content is often shown to provoke strong reactions.

Supporting your child

- Play “spot the fake” games using examples of false headlines.
- Encourage them to verify images (Google reverse image search).
- Teach them to ask: Who benefits if I believe this?

When things go wrong

If your child starts believing conspiracy theories or spreading false claims:

- Avoid direct confrontation – ask questions to encourage self-reflection.
- Provide reliable sources at their level (e.g., youth-friendly health sites).
- Seek advice if beliefs disrupt relationships or schoolwork.

Suggested reading

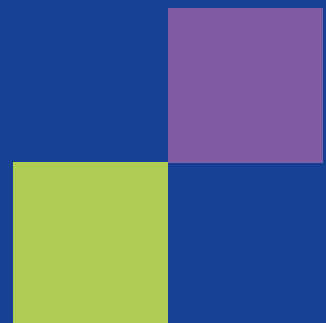
- Wardle, C. & Derakhshan, H. (2017). Information Disorder. Council of Europe Report.

(https://edoc.coe.int/en/module/ec_addformat/

download?cle=5905aa3361a00b7d9356fa6cf222396d&k=986230e363ed790f7583165280237884)

CHAPTER 3

RESILIENCE BUILDING



WHAT IS RESILIENCE IN THE DIGITAL AGE?

Resilience is the ability to cope with challenges, recover from setbacks, and adapt to change. In the digital world, resilience has an added dimension: helping children and adolescents handle the ups and downs of online life.

The internet can be a wonderful space for learning, connection, and creativity. Yet it can also expose young people to cyberbullying, exclusion, harmful content, or pressure to meet unrealistic standards. Resilience doesn't mean avoiding these challenges entirely – that's impossible. Instead, it's about equipping children with the skills and emotional strength to navigate difficulties without being overwhelmed.

For parents and carers, resilience is also about supporting your child emotionally, creating safe spaces for discussion, and modelling healthy coping strategies yourself.

Why Resilience Matters for Children and Adolescents

Children and young people spend significant parts of their lives online. They build friendships, explore identities, learn new skills, and encounter new ideas in digital spaces. These experiences are often positive, but challenges are inevitable.

Common online stressors include:

- Cyberbullying or exclusion from online groups.
- Exposure to distressing images or harmful content.
- Comparison with “perfect” lives shown on social media.
- Pressure to be constantly available and responsive.
- Overwhelm from information overload.

Without resilience, these challenges can lead to:

- Anxiety and low self-esteem.
- Withdrawal from friendships or activities.
- Difficulty concentrating at school.
- Risk-taking behaviours online.

Resilience acts as a protective factor, reducing the likelihood that negative experiences will cause long-term harm.

DEVELOPING YOUR OWN RESILIENCE AS A PARENT OR CARER

Before you can support your child, it helps to strengthen your own digital resilience. Children often mirror how adults respond to stress, so your coping strategies matter.

1. Recognise Your Own Digital Stress

Parents face digital pressures too – work emails at all hours, worrying news cycles, or pressure to appear “perfect” online. Take time to notice how these affect your mood and behaviour.

2. Model Healthy Coping

Show your child what it looks like to respond calmly to digital challenges:

- If a message upsets you, explain that you’re taking a break before replying.
- If you feel anxious about news, say you’ll check a trusted source and then step away.
- If you’re frustrated by technology, show patience instead of anger.

3. Build Family Habits That Support Balance

Simple routines like device-free meals, shared outdoor time, or agreed “switch-off” hours demonstrate that digital life should be part of a balanced lifestyle, not dominate it.

SUPPORTING YOUR CHILD'S RESILIENCE

1. Create a Safe Space for Conversations

Make it clear that your child can talk about their online experiences without fear of punishment. For example, if they encounter harmful content, they should feel confident that you will listen and help, not immediately ban their device.

2. Teach Emotional Awareness

Help your child recognise how online experiences affect their feelings:

- How do you feel when you see lots of perfect holiday photos?
- What emotions come up when someone ignores your message?

Naming emotions is the first step in managing them.

3. Encourage Healthy Coping Strategies

- Taking breaks from screens when overwhelmed.
- Talking to a trusted adult or friend.
- Engaging in offline hobbies to balance digital time.
- Using relaxation techniques like deep breathing.

4. Build Positive Online Communities

Encourage your child to engage in digital spaces that promote creativity, kindness, and learning. Being part of supportive communities can strengthen resilience against negative experiences.

WHEN THINGS GO WRONG

Even with support, your child may face serious digital challenges. The way you respond can make a big difference.

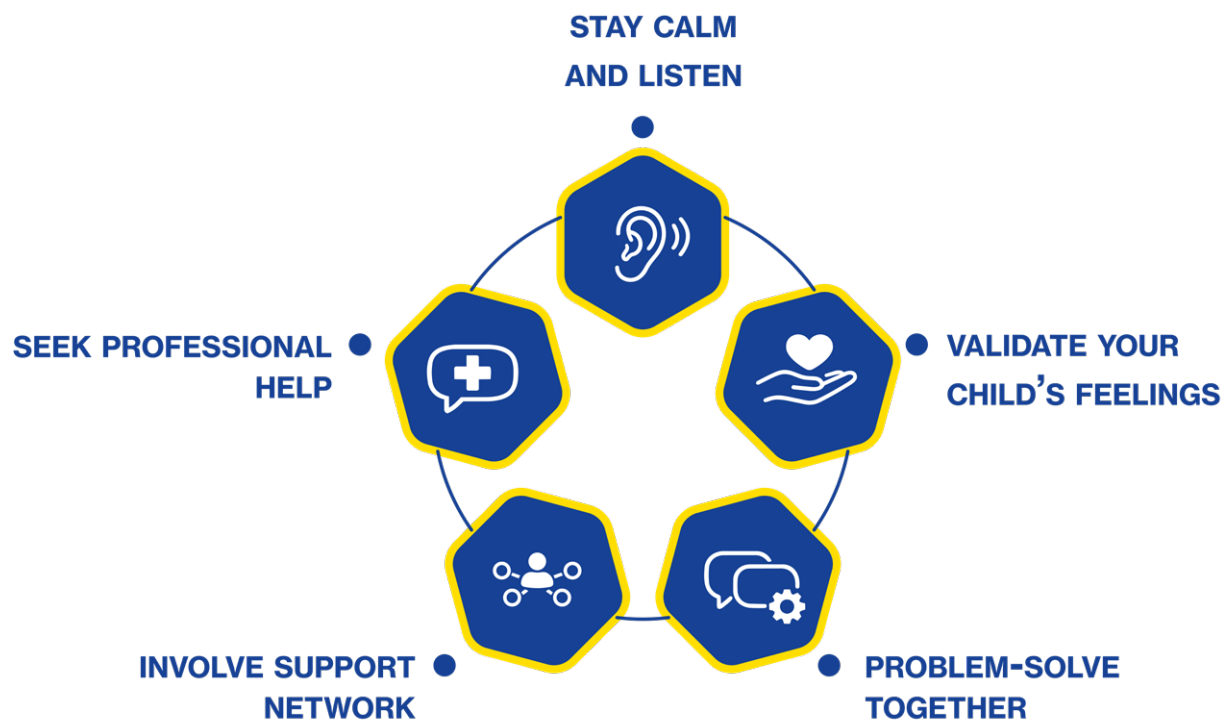
Warning Signs of Struggling Resilience

- Withdrawal from online and offline social life.
- Sudden changes in mood after online activity.
- Reluctance to use devices they previously enjoyed.
- Obsession with negative content or online conflicts.
- Physical symptoms like trouble sleeping or headaches.

How to Respond

1. **Stay Calm and Listen:** Create space for your child to share what happened. Avoid immediate judgment or problem-solving; begin by listening.
2. **Validate Their Feelings:** Say things like: “That sounds really tough” or “I understand why you feel upset.” Validation helps your child feel understood and less alone.
3. **Problem-Solve Together:** Ask: “What would help you feel better? Do you want to report this? Should we take a break together?” Collaborating builds empowerment.
4. **Involve Support Networks:** If needed, involve teachers, school counsellors, or support organisations. Many schools now have clear processes for addressing online bullying or distress.
5. **Seek Professional Help if Necessary.** If your child shows signs of prolonged anxiety, depression, or self-harm thoughts, seek professional support from a GP, counsellor, or mental health specialist.

HOW TO RESPOND IF YOUR CHILD STRUGGLES WITH RESILIENCE





CASE STUDY 1: EXCLUSION FROM A GROUP CHAT

A 12-year-old is removed from a class WhatsApp group without explanation. They feel humiliated and isolated. The parent listens calmly and reassures them that their feelings are valid. Together, they talk about online group dynamics and brainstorm supportive friends to connect with offline. The parent also contacts the teacher discreetly to monitor class social dynamics.

CASE STUDY 2: EXPOSURE TO DISTURBING CONTENT

A teenager accidentally views violent images shared by peers. They become withdrawn and anxious. Instead of banning their phone, the parent encourages open discussion about what they saw and why it was distressing. They review privacy settings and reporting tools together, then balance screen time with calming offline activities. Over time, the teen feels more in control and less fearful.

CASE STUDY 3: SOCIAL MEDIA PRESSURE

A 14-year-old constantly compares themselves to influencers on social media, leading to low self-esteem. The parent initiates a conversation: "Do you think these images show real life? What might be edited?" They encourage the teen to follow positive role models and take breaks when posts trigger negative feelings. Gradually, the teen becomes more selective in their online environment.

PRACTICAL TOOLS FOR PARENTS

Family Resilience Habits

- Device-free dinners.
- One daily offline activity together (walk, game, reading).
- Encourage “pause and reflect” before responding to upsetting content.
- Regular check-ins: “How are you feeling about online stuff this week?”

Conversation Starters

- What’s the best thing that happened to you online this week?
- What’s the hardest thing?
- Who online makes you feel good about yourself?
- When you feel upset online, what helps you calm down?

Coping Strategy Checklist for Children

- Take a short break from the screen.
- Talk to a parent, teacher, or friend.
- Use “report” or “block” functions.
- Write feelings down or draw them.
- Do something relaxing offline (music, drawing, sport).

The Resilience Roadmap

Helping families cope, recover, and grow stronger in the digital age.

Stage 1: Awareness

Goal: Recognise that challenges online are normal and that resilience can be learned.

- Talk openly about both positive and negative online experiences.
- Share your own examples of mistakes and recovery (e.g., falling for a scam email, feeling upset by social media).
- Teach children that setbacks are part of learning, not signs of failure.

Red Flags:

- Child says “I’m stupid” or “I can’t handle this.”
- Avoidance of digital spaces after a single negative experience.

Checklist:

- I talk about my own digital ups and downs. ☐
- My child knows mistakes online are not the end of the world. ☐
- We discuss both risks and opportunities of being online. ☐

Stage 2: Coping Skills

Goal: Give children tools to manage stress and negative emotions when things go wrong online.

Practical Tools:

- The 5-Step Pause: Stop – Breathe – Think – Choose – Act.
- Encourage “digital breaks” (walk, stretch, do something offline).
- Teach grounding strategies: naming 5 things they see, 4 they feel, 3 they hear.
- Role-play: “What would you do if someone posted something mean?”

Red Flags:

- Emotional outbursts after online use.
- Reluctance to share what’s happening online.
- Withdrawal from friends or activities.

Checklist:

- My child can name at least one coping technique. ☐
- We practise “taking a break” when things feel overwhelming. ☐
- I encourage calm responses instead of quick reactions online. ☐

Stage 3: Support Networks

Goal: Ensure children know they are not alone and can turn to trusted people.

Actions for Parents:

- Identify safe adults (parents, teachers, relatives) your child can talk to.
- Normalise asking for help: “Even adults need help online sometimes.”
- Connect with other parents to share strategies and coordinate approaches.

Red Flags:

- Child hides online activity and refuses to talk about problems.
- They believe nobody would understand or help.

Checklist:

- My child can name at least 2 safe adults they could approach. ☐
- We have regular “digital check-ins” (casual chats about online life). ☐
- I model asking for advice myself, so my child sees it’s normal. ☐

Stage 4: Recovery

Goal: Move from crisis to healing after an incident (bullying, hacking, exposure to harmful content).

Steps for Parents:

1. Stay Calm: Avoid blame or panic.
2. Validate: “I can see this was really upsetting.”
3. Act Together: Block/report accounts, reset passwords, or contact school if needed.
4. Rebuild Confidence: Encourage positive online activities (creative projects, safe games).

Red Flags:

- Ongoing distress long after the incident.
- Withdrawal from online life entirely.
- Declining grades, sleep, or friendships.

Checklist:

- I focus on solutions, not punishment. ☐
- We act together to fix problems. ☐
- I help my child return to positive digital use. ☐

Stage 5: Growth

Goal: Turn challenges into learning experiences that build long-term resilience.

Strategies:

- Reflect together: “What did we learn from this?”
- Encourage your child to help others with their experiences.
- Celebrate small wins (reporting a scam, blocking a bully, resisting pressure to overshare).

Red Flags:

- Child continues to see themselves as a “victim” without recognising growth.
- They avoid reflecting or deny learning from experiences.

Checklist:

- We talk about what we learned from digital challenges. ☐
- My child has shared their skills or advice with someone else. ☐
- We celebrate resilience, not just success. ☐

Family Resilience Agreement

Write down and display your family's core resilience principles:

1. We talk openly about online experiences.
2. We take breaks when things get overwhelming.
3. We always ask for help if we need it.
4. We act together to fix problems.
5. We treat mistakes as learning opportunities.

Quick "Resilience in Action" Guide

- When upset: Stop – Breathe – Talk – Act.
- When unsure: Ask, check, verify.
- When things go wrong: No blame, fix it together.
- When recovered: Reflect and share what you learned.

CONCLUSION

Resilience is not about shielding children from all negative experiences. Instead, it is about helping them develop the skills, confidence, and emotional strength to navigate challenges. As a parent or carer, you play a crucial role in this process: by modelling calm responses, creating open spaces for dialogue, and equipping your child with practical strategies. When setbacks occur, treat them as opportunities for growth, not failures. The DRONE project emphasises that resilience is a shared journey. Children, parents, schools, and communities all contribute to building stronger, safer digital environments. By focusing on resilience, you are not only helping your child cope with online difficulties but also giving them tools that will serve them throughout their lives.

Why it matters

Children exposed to negative online experiences – mockery, exclusion, disturbing content – need emotional tools to cope. Resilience does not mean avoiding all risks but managing them constructively.

Supporting resilience

- Encourage daily screen breaks and physical activity.
- Promote open family conversations about online life.
- Share your own experiences of mistakes and recovery online.

For your child's mental well-being

- Teach “digital first aid”: stop, breathe, talk, report, and recover.
- Encourage critical distance: “Not everything online is about you.”
- Support peer networks – friends can be protective factors.

When things go wrong

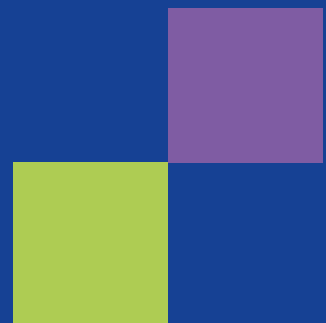
- Look out for withdrawal, anxiety, or obsessive online checking. Steps include:
- Listen non-judgmentally.
- Contact teachers or counsellors.
- Use professional resources if distress escalates.

Suggested reading:

- Livingstone, S. & Byrne, J. (2018). Parenting in the Digital Age.
- Common Sense Media: “Digital Well-Being” guides. (<https://www.commonsensemedia.org/digital-well-being>)

CHAPTER 4

PROBLEM-SOLVING



WHAT IS PROBLEM-SOLVING IN THE DIGITAL AGE?

Problem-solving is the ability to recognise challenges, generate solutions, and make decisions that are thoughtful and effective. In the digital world, problem-solving is not just about fixing a broken app or figuring out a new device. It's about responding to complex issues like:

- A child receiving hurtful messages in a group chat.
- Being locked out of an account.
- Deciding whether to trust a website asking for personal information.
- Navigating conflicts in online games.

These situations can be confusing and stressful for both children and parents. Strong problem-solving skills help families approach digital challenges calmly and constructively, rather than reacting with panic or avoidance.

Why Problem-Solving Matters for Parents and Carers

Children and adolescents are still learning how to make decisions and handle unexpected issues. As a parent or carer, your problem-solving skills influence how your child learns to manage their own. If you respond to a digital challenge with anger or fear, they may copy that response. If you model calm analysis and thoughtful choices, they are more likely to develop those habits themselves.

In practice, this means:

- Equipping yourself first: Learn the steps of effective problem-solving so you feel confident when digital issues arise.
- Guiding your child: Teach them a process they can use when challenges come up.
- Supporting without taking over: Encourage independence while being available for help when needed.

DEVELOPING YOUR OWN PROBLEM-SOLVING SKILLS

1. Pause Before Reacting

Digital problems can provoke strong emotions. Before acting, take a moment to breathe and assess. Ask yourself: What is actually happening? What do I need to know before I respond?

2. Break the Problem Down

Define the issue clearly. For example, instead of “My child is unsafe online,” identify: “My child is receiving anonymous hurtful messages on Instagram.” Breaking the issue into specifics makes it easier to address.

3. Generate Options

Brainstorm possible solutions without immediately judging them. For example: block the sender, report the account, change privacy settings, talk to the school, or support your child emotionally.

4. Weigh Pros and Cons

Consider the likely outcomes of each option. Blocking might solve the immediate issue but not address the emotional impact. Reporting may take longer but helps prevent future harm.

5. Take Action and Reflect

Choose the best option, act on it, and later reflect: Did it work? What could we do differently next time?

By practising these steps yourself, you can guide your child through them when challenges arise.

SUPPORTING YOUR CHILD'S PROBLEM-SOLVING

1. Teach a Simple Framework

You don't need to give children a lecture on decision-making theory. Instead, introduce a simple, memorable process like:

STOP – THINK – CHOOSE – CHECK

- STOP: Pause before reacting.
- THINK: What's really happening? What are the options?
- CHOOSE: Pick the best option.
- CHECK: Did it work? Do I need to try again?

2. Practise With Small Issues

Help your child practise problem-solving in everyday digital situations:

- Forgotten a password? Work together to reset it.
- Uncertain about downloading a new app? Review permissions and reviews together.
- Unsure if a message is a joke or what it means? Role-play possible responses.

3. Encourage Independence

As children get older, resist the urge to fix every problem immediately. Instead, ask guiding questions:

- What do you think is the best way to handle this?
- What are the risks and benefits of that choice?
- How could you prevent this from happening again?

4. Provide Emotional Support

Problem-solving is not just technical. Digital problems often have emotional consequences. Validate your child's feelings before moving to practical solutions.

WHEN THINGS GO WRONG

Not every problem can be solved smoothly. Sometimes situations escalate despite your best efforts.

Warning Signs of Escalating Digital Problems

- Repeated or worsening bullying despite blocking/reporting.
- A child obsessing over an online conflict.
- Financial risks, such as in-game purchases or scams.
- Emotional distress linked to digital challenges.

How to Respond

1. Reassure Your Child

Let them know that all problems have solutions, even if they take time.

2. Seek External Support

Contact teachers, school staff, or online platform moderators if the issue is beyond your control.

3. Learn From the Experience

Ask: What worked? What didn't? What could we try next time? This turns setbacks into valuable learning.

4. Address Emotional Impact

If your child is anxious, ashamed, or withdrawn, focus first on their well-being before addressing technical fixes.

HOW TO RESPOND WHEN YOUR CHILD FACES ESCALATING DIGITAL PROBLEMS

REASSURE YOUR CHILD ●



● SEEK EXTERNAL SUPPORT



LEARN FROM EXPERIENCE ●



● ADDRESS EMOTIONAL IMPACT





CASE STUDY 1: THE GAMING CONFLICT

A 10-year-old gets into a heated argument in an online game, leading to name-calling and exclusion from a team. The child is devastated. Instead of forbidding the game, the parent guides them through problem-solving:

- Stop: Take a break from the game.
- Think: What happened? (A disagreement about strategy escalated.)
- Choose: Apologise privately and suggest a new game with different friends.
- Check: Did it improve the situation? (Yes, the child reconnected with a different group.)

The child learns that digital conflicts can be managed with calm choices.

CASE STUDY 2: THE SUSPICIOUS EMAIL

A teenager receives an email claiming they have won a prize and asks for personal details. Excited, they show it to their parent. Instead of scolding, the parent guides them through evaluation:

- Who sent this? Is the email address genuine?
- Why would someone give away money to strangers?
- What happens if we click the link?

Together, they identify it as a scam. The teen feels proud for spotting it and becomes more cautious with emails.

CASE STUDY 3: THE SOCIAL MEDIA DILEMMA

A 14-year-old feels pressured to join a private group where peers share content that seems unkind. Unsure what to do, they ask a parent. Instead of deciding for them, the parent asks:

- What are the risks of joining?
- How would you feel if you were the one being made fun of?
- What other options do you have?

The teen chooses not to join and explains to friends that they don't feel comfortable. They gain confidence in making values-based decisions.

PRACTICAL TOOLS FOR PARENTS

Problem-Solving Checklist

- Did I pause before reacting? ☐
- Did I define the problem clearly? ☐
- Did I consider at least two options? ☐
- Did I think about the risks and benefits? ☐
- Did I reflect afterwards? ☐

Family “What If” Scenarios

Once a week, discuss a digital “what if” together:

- What if someone you don’t know asks for personal info?
- What if a game friend starts being mean?
- What if you see something upsetting online?

Talk through or role play possible responses.

Encouraging Independence

- Use guiding questions instead of giving immediate answers.
- Celebrate effort and good judgment, even if outcomes aren’t perfect.
- Remind your child that mistakes are part of learning.

Define, Explore, Act, Reflect (DEAR) - a structured approach to problem-solving

- Define: Identify the real problem beneath symptoms.
- Explore: Brainstorm possible solutions and evaluate them.
- Act: Choose and plan a realistic solution.
- Reflect: Review the process, learn, and adjust.

CONCLUSION

Problem-solving is one of the most important skills your child can develop in the digital age. It helps them face challenges with confidence, creativity, and resilience.

As a parent or carer, your role is to:

1. Strengthen your own problem-solving skills so you can model calm, thoughtful responses.
2. Guide your child by teaching simple frameworks they can remember and apply.
3. Support without taking over, encouraging independence and reflection.

When problems escalate, treat them as opportunities for learning and growth. The goal is not to shield your child from every difficulty but to help them build the tools they need to navigate digital challenges throughout life.

For parents

Digital problem-solving means troubleshooting technical issues, but also navigating complex situations (e.g., privacy breaches).

For children

Problem-solving skills include deciding whether to respond to a message, how to resolve peer conflicts online, or how to manage time across apps.

How to support

- Practise scenarios: “What would you do if someone shared your photo without permission?”
- Encourage children to think through options and outcomes.
- Reinforce that asking for help is part of problem-solving.

When things go wrong

If a digital problem becomes overwhelming:

- Break it down into smaller steps.
- Involve your child in the solution.
- Seek technical or professional help if necessary.

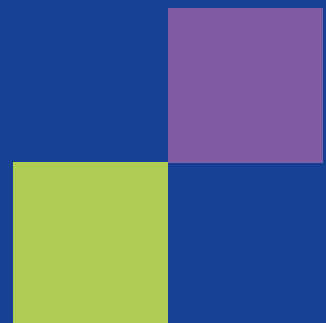
Suggested reading

- Gee, J.P. (2017). Teaching, Learning, Literacy in Our High-Risk High-Tech World. ³

³ https://www.researchgate.net/publication/344569053_Teaching_learning_literacy_in_our_high-risk_high-tech_world_A_framework_for_becoming_human_2017_By_J_P_Gee_Teachers_College_Press_184_pages_ISBN_978-0-8077-5860-1

CHAPTER 5

CRITICAL THINKING



Developing Your Own Critical Thinking Skills

1. Notice Your Own Assumptions

We all carry biases that affect how we interpret information. Ask yourself: Am I believing this because it fits my opinion, or because it's supported by evidence?

2. Practise Every day Questioning

When you read an article, see a meme, or hear a rumour, practise asking:

- Who said this?
- What evidence do they provide?
- What might they gain from me believing this?
- What voices are missing?

3. Be Comfortable with Uncertainty

Critical thinking is not about having all the answers. Sometimes the best response is: I don't know yet. Let's look into it together. Modelling curiosity and openness shows your child that uncertainty is normal.

Supporting Your Child's Critical Thinking

1. Encourage Questions

Welcome your child's curiosity, even if their questions are challenging. Instead of giving immediate answers, explore together. For example:

- That's an interesting claim. Where could we check if it's true?
- Why do you think someone might post that?

2. Use Real-Life Examples

Use news stories, adverts, or social media posts as practice material. Discuss together:

- Is this fact or opinion?
- How does this content make us feel?
- Who benefits if we believe this?

3. Promote Respectful Debate

Encourage your child to express their opinions and listen to others. Teach them that disagreeing respectfully is a strength, not a weakness.

4. Teach “Slow Thinking”

Children often scroll quickly and react instantly. Encourage them to slow down. Even a short pause before liking, sharing, or commenting allows space for reflection.

WHEN THINGS GO WRONG

Sometimes children will struggle with critical thinking. They may:

- Believe conspiracy theories.
- Accept stereotypes or harmful claims without questioning.
- Argue strongly without evidence.
- Resist considering other viewpoints.

Warning Signs

- Frequent repetition of extreme claims.
- Dismissing evidence without engaging with it.
- Becoming defensive when challenged.
- Spreading harmful content without checking.

How to Respond

1. Stay Calm

Avoid ridiculing or shaming. Instead, ask open-ended questions.

2. Explore Together

Rather than saying, “That’s wrong,” say: “Let’s see what other sources say. How can we check this?”

3. Model Humility

Admit when you don’t know something. This shows that questioning and learning are ongoing processes.

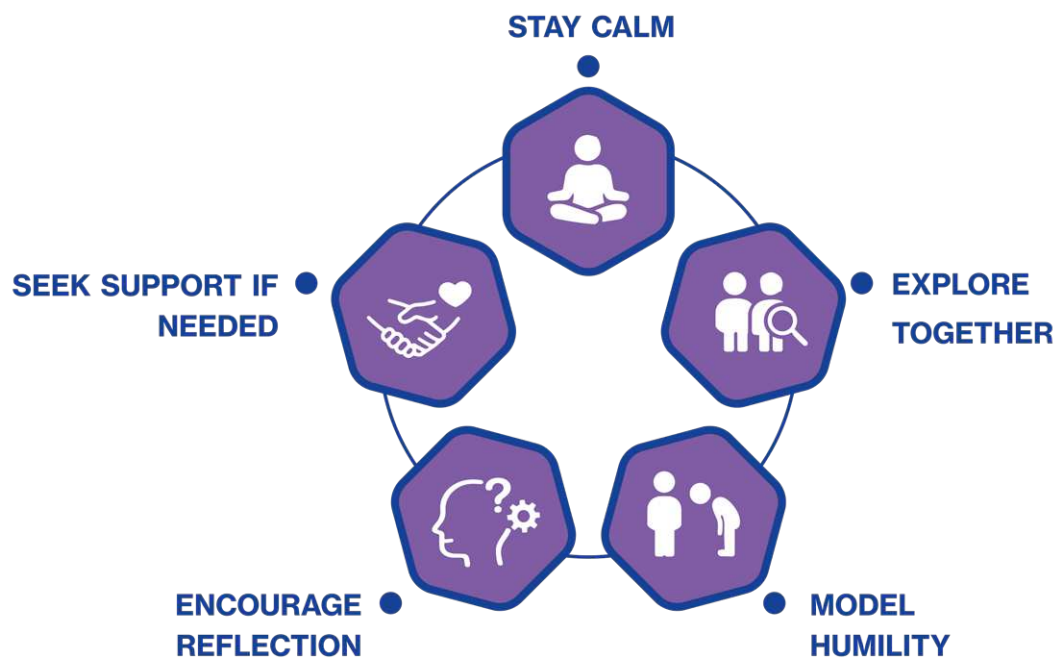
4. Encourage Reflection

Ask: “What made this believable to you? What would convince you otherwise?”

5. Seek Support If Needed

If your child is drawn into harmful ideologies or online groups, seek professional advice or talk to their teachers. Schools may be able to integrate critical thinking into classroom discussions.

HOW TO RESPOND IF YOUR CHILD STRUGGLES WITH CRITICAL THINKING





CASE STUDY 1: THE VIRAL VIDEO

A 13-year-old insists a viral video proves a wild claim about health. The parent resists dismissing it outright and instead says: "Let's check where this video came from. Who made it? What do experts say?" Together, they find that the video was taken out of context. The child learns that visuals can be powerful but misleading.

CASE STUDY 2: THE STEREOTYPE

An 11-year-old repeats a harmful stereotype heard online. Instead of scolding, the parent asks: "Where do you think that idea comes from? Does it apply to everyone? How would you feel if someone said that about you?" The child begins to see that stereotypes are unfair and oversimplified.

CASE STUDY 3: THE DEBATE AT SCHOOL

A teenager comes home after a heated debate with classmates about climate change. They are frustrated that some peers deny scientific evidence. The parent helps them practise respectful debate skills: acknowledging others' feelings, presenting evidence clearly, and knowing when to disengage. This boosts their confidence and resilience in future discussions. The parent also contacts the class teacher and suggests implementing exercises in class that builds debate culture.

Practical Tools for Parents

Everyday Critical Thinking Prompts

- Is this fact, opinion, or persuasion?
- What's the evidence?
- Who gains if I believe this?
- What information might be missing?
- How does this make me feel – and why?

Family Discussion Ideas

- Compare two news articles on the same event. What's similar? What's different?
- Watch a YouTube video and discuss: fact, opinion, or entertainment?
- Explore an advertisement: how does it try to persuade us?

Critical Thinking Habits to Model

- Admit when you don't know something.
- Share your own thought process aloud: "I'm not sure about this claim. Let's check another source."
- Show openness to changing your mind when new evidence appears.

Conclusion

Critical thinking is one of the most powerful tools parents can give children in the digital age. It helps them:

- Question information rather than accept it blindly.
- Recognise persuasion and manipulation.
- Engage respectfully with different viewpoints.
- Develop independence and confidence in decision-making.

For parents and carers, the journey begins with strengthening your own critical thinking habits. By modelling curiosity, openness, and humility, you create a home environment where questioning is welcomed, and learning is shared.

When challenges arise, treat them as learning opportunities. Every debate, stereotype, or viral myth is a chance to practise the art of critical thinking.

The DRONE project highlights that parents and carers are not just supervisors of digital use but active mentors. By cultivating critical thinking together, you help your child grow into an informed, thoughtful, and resilient digital citizen.

Supporting your child

- Ask them: “What evidence supports this?”
- Compare news from different perspectives.
- Use debates to practise respectful disagreement.

When things go wrong

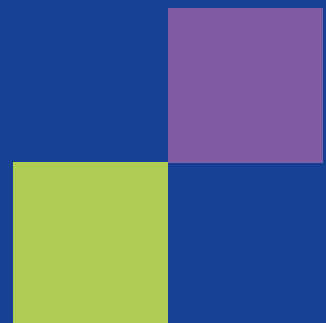
- If your child struggles with extreme or manipulative ideas:
- Stay curious – ask, don’t lecture.
- Share age-appropriate resources that present balanced evidence.
- Engage with teachers to encourage critical engagement across subjects.

Suggested reading:

- Paul, R. & Elder, L. (2019). Critical Thinking: Tools for Taking Charge of Your Learning and Your Life. (<https://dn790004.ca.archive.org/0/items/critical-thinking-tools-for-taking-charge-of-your-professional-life-2e/Critical%20Thinking%20-%20Tools%20for%20Taking%20Charge%20of%20Your%20Professional%20Life%202e.pdf>)

CHAPTER 6

BULLYING AND CYBERBULLYING



UNDERSTANDING BULLYING IN ALL ITS FORMS

Bullying is a pattern of repeated, intentional behaviour aimed at causing harm, distress, or humiliation to another person. In the digital age, this can happen both face-to-face and online (cyberbullying).

While media stories often highlight cases of peer bullying, evidence shows that other forms of bullying are often more common and more damaging:

- Teacher-to-student bullying, where authority figures use humiliation, sarcasm, threats, or unfair treatment.
- Bullying by family members, including siblings, cousins, or even parents who use belittling, controlling, or shaming behaviours.
- Peer bullying, while real, is often less frequent than assumed but still deserves attention.

Recognising these realities is important because children are often reluctant to report bullying when it comes from adults they are supposed to trust, or from close family.

WHY BULLYING BY ADULTS IS SO HARMFUL

1. Bullying by Teachers or School Staff

Children look to teachers for safety, guidance, and learning. When teachers use their authority to belittle, intimidate, or unfairly punish, the impact can be profound:

- Loss of trust in school as a safe place.
- Lasting harm to self-esteem and motivation.
- Fear of speaking up or asking questions.

Examples include:

- Publicly mocking a student's mistakes.
- Singling out one child for constant criticism.
- Ignoring bullying by peers as a form of punishment.

2. Bullying by Family Members

Bullying at home is often minimised or dismissed as “teasing” or “discipline.” But repeated patterns of humiliation, comparison, or control are harmful:

- Constant criticism (“Why can’t you be like your brother?”).
- Using shame as punishment (“You’re useless, no one will like you.”).
- Exclusion from family activities.

Family bullying is especially painful because children often cannot escape it, and they may feel guilty for resenting those they are expected to love.

3. Peer Bullying (Including Online)

Peer bullying does occur, particularly in digital spaces where anonymity gives children a sense of power. Forms include:

- Hurtful comments in group chats.
- Exclusion from online games or groups.
- Spreading rumours on social media.

Although less common than adult-driven bullying, peer bullying can still cause real distress and requires careful attention.

Cyberbullying in Context

Cyberbullying magnifies bullying's impact because:

- It can happen at any time, leaving no safe space.
- Hurtful messages or images can be shared widely and quickly.
- Victims may not know who the bully is (especially with anonymous accounts).
- Digital traces make it feel permanent, even when posts are deleted.

Cyberbullying may be carried out by peers, but it can also occur through adults misusing digital platforms (for example, teachers humiliating students in class WhatsApp groups or parents shaming children publicly online).

Recognising the Signs

Signs Your Child May Be Bullied (by adults or peers):

- Sudden changes in mood after school or family gatherings.
- Reluctance to attend school or family events.
- Unexplained headaches, stomach aches, or trouble sleeping.
- Withdrawal from digital devices or, conversely, constant checking of them.
- Repeating negative statements said by others ("I'm stupid," "Nobody likes me").

Signs of Cyberbullying:

- Anxiety when receiving notifications.
- Deleting or hiding screens quickly when you enter the room.
- Sudden changes in online activity (e.g., deleting accounts).
- Emotional distress after being online.

SIGNS THAT YOUR CHILD MAY BE EXPERIENCING BULLYING



1

**MOOD
CHANGES**



2

**RELUCTANCE
TO ATTEND
SCHOOL OR
FAMILY
EVENTS**



3

**UNEXPLAINED
ACHES,
SLEEPING
TROUBLE**



4

**AVOIDING/
CONSTANTLY
CHECKING
DIGITAL
DEVICES**



5

**REPEATING
NEGATIVE
STATEMENTS**

SUPPORTING YOUR CHILD

1. Listen Without Judgment

Children are often reluctant to report bullying – especially when it comes from teachers or family members. Reassure them: “You can tell me anything. I’ll listen, and we’ll figure it out together.”

2. Validate Their Experience

Avoid minimising. Instead of “It can’t be that bad,” say: “I can see this is hurting you. Thank you for telling me.”

3. Empower Them with Options

Ask: “What would make you feel safer? What should we do next?” Options might include talking to the school, blocking accounts, or seeking professional support.

4. Model Respectful Boundaries

Show your child that nobody – not even a teacher or family member – has the right to humiliate them. Reinforce the idea that respect should be mutual.

WHEN THINGS GO WRONG

Bullying by Teachers or School Staff

Document Incidents: Write down dates, times, and behaviours. Save digital messages if applicable.

1. **Communicate with Care:** Contact the school leadership calmly but firmly, using evidence.
2. **Escalate if Needed:** If the school does not act, escalate to education authorities or ombudsman services.
3. **Support Your Child's Confidence:** Remind them that poor treatment is about the teacher's behaviour, not their worth.

Bullying by Family Members

Address Directly but Calmly: If safe, talk to the family member about the harm caused.

1. **Set Boundaries:** Limit contact if bullying continues.
2. **Protect Emotional Safety:** Prioritise your child's well-being over family pressure to "keep the peace."

Peer Cyberbullying

Pause Before Reacting: Don't immediately remove devices; this can feel like punishment.

1. **Use Tools:** Block, mute, or report accounts.
2. **Involve the school only if it happened at school:** Most schools have anti-bullying policies, but parents need to make sure the problem is not escalated by asking them to get involved.
3. **Focus on Recovery:** Encourage positive online and offline experiences to rebuild self-esteem.



CASE STUDY 1: TEACHER HUMILIATION

A 9-year-old is regularly mocked by a teacher for “always being slow.” The child becomes anxious and refuses to go to school. The parent documents incidents, meets with the headteacher, and advocates for respectful classroom practices. The teacher receives support and supervision, and the child’s anxiety decreases.

CASE STUDY 2: FAMILY CRITICISM

An uncle constantly calls a teenager “lazy” and “worthless” at family gatherings or in the family chat group. The teen withdraws socially. The parent intervenes, explains that such comments are harmful, and sets a boundary: the uncle may not speak to the teen that way. The family dynamic shifts, and the teen feels protected.

CASE STUDY 3: GROUP CHAT EXCLUSION

A 12-year-old is excluded from a class group chat, and cruel messages circulate. Instead of banning their phone, the parent listens, helps them block the chat, and contacts the school discreetly. The school facilitates restorative conversations. The child learns that exclusion does not define their worth.

PRACTICAL TOOLS FOR PARENTS

Bullying Red Flags Checklist

- My child expresses dread about school or family events. ☐
- They seem anxious or upset after being online. ☐
- They withdraw from friends or activities. ☐
- They use self-blaming language. ☐
- They resist talking about experiences that clearly bother them. ☐

Parent Action Plan

- Listen first, without judgment.
- Validate their feelings.
- Document incidents clearly.
- Identify safe adults (in school or extended networks).
- Take action (school meetings, boundaries at home, reporting tools).
- Support emotional recovery with encouragement and positive activities.

Family Conversation Starters

- Has anyone ever made you feel small or embarrassed on purpose?
- How do you know the difference between teasing and bullying?
- What should you do if a teacher or adult treats you unfairly?
- How can I support you if something like this happens again?

Parent Toolkit: Responding to Bullying

Bullying can come from many directions – not only peers but also teachers and even family members. This toolkit gives you concrete steps to support your child and take action.

General Principles

- Stay calm – your reaction teaches your child how to respond.
- Listen without judgment – let your child share in their own words.

- Reassure – remind them bullying is never their fault.
- Document – write down what happened, when, and who was involved.
- Act – take steps appropriate to the situation, rather than ignoring it.

1. If Your Child Is Bullied by a Teacher

Warning Signs

- Fear of school or a particular class.
- Frequent stomach aches or headaches on school days.
- Reports of humiliation, unfair treatment, or name-calling from staff.

Steps to Take

1. Listen and Validate
 - Believe your child.
 - Avoid dismissing behaviour as “strict teaching.”
2. Document Incidents
 - Record dates, times, witnesses, and what was said or done.
3. Talk With Your Child About Desired Outcomes
 - Do they want the bullying to stop quietly?
 - Do they want a change of teacher or an apology?
4. Escalate in Steps
 - First: arrange a meeting with the teacher.
 - If unresolved: contact the headteacher/principal.
 - If still unresolved: escalate to the school board or education authority.
5. Provide Emotional Support
 - Remind your child that authority figures are not always right.
 - Offer counselling support if needed.

Checklist

- I have documented incidents with detail. ☐
- I spoke calmly with my child about how they want me to act. ☐
- I know the school’s complaint policy. ☐
- I am prepared to escalate if needed. ☐

2. If Your Child Is Bullied by a Family Member

Warning Signs

- Reluctance to visit or interact with certain relatives.
- Sudden changes in mood after family gatherings.
- Being targeted with constant criticism, mocking, or exclusion.

Steps to Take

1. Acknowledge the Issue
 - Don't excuse harmful behaviour as "family jokes."
2. Create Safe Boundaries
 - Limit or supervise contact with the relative.
 - Make clear rules: respect is non-negotiable.
3. Address Directly if Safe
 - Speak with the family member about the behaviour.
 - Use "I" statements (e.g., "I cannot allow you to talk to my child this way").
4. Protect Your Child's Wellbeing
 - Prioritise safety over family harmony.
 - If necessary, cut contact.
5. Seek External Support
 - Family counselling.
 - Child protection services if behaviour is abusive.

Checklist

- I have listened to my child and validated their feelings. ☐
- I set clear boundaries with relatives. ☐
- I have considered whether continued contact is healthy. ☐
- I sought professional help if bullying became abusive. ☐

3. If Your Child Is Bullied by a Peer

Warning Signs

- Avoidance of social activities.
- Sudden drop in grades.
- Reluctance to use devices (if cyberbullying) or constant checking.

Steps to Take

1. Listen and Support
 - Tell your child: “You did the right thing by telling me.”
2. Document Incidents
 - Save screenshots, messages, or witness reports.
3. Help Your Child Respond Safely
 - Encourage blocking and reporting, not retaliation.
 - Practise assertive but safe responses.
4. Contact the School
 - Share documentation with staff.
 - Ask for the anti-bullying policy to be applied.
5. Monitor Emotional Health
 - Watch for withdrawal, depression, or anxiety.
 - Seek counselling if needed.

Checklist

- I have saved evidence of bullying.
- I coached my child on safe responses.
- Did it happen at school? If yes, I contacted the school to address the issue.
- I checked in regularly on my child’s well-being.

4. When to Seek Immediate Help

- Your child talks about self-harm or suicide, or shows signs of self-harm (e.g. cutting).
- Bullying includes physical abuse.
- The school or family environment ignores or covers up the problem.

Who to Contact

- Professional mental health specialists or friends you trust.
- Child protection services.
- National helplines (Childline, Kids Helpline, etc.).
- Mental health crisis lines.

Conversation Starters with Your Child

- “What happened today that made you feel good? What about something that upset you?”
- “If someone is unkind, how does it make you feel? What would you want me to do?”
- “Remember, nothing you tell me will get you in trouble. I’m here to help.”

CONCLUSION

Bullying in the digital age is a serious issue, but it is not always where parents expect to find it. While peer bullying does occur, the more common and damaging sources are often teachers, school staff, and family members. These situations are harder for children to talk about because they involve authority figures or loved ones.

As a parent or carer, your role is to:

1. Acknowledge all forms of bullying, not just peer-to-peer.
2. Create safe spaces for disclosure where your child knows you will listen and protect them.
3. Model boundaries and advocacy, showing that even adults can be held accountable for poor behaviour.
4. Support recovery, not only by addressing the incidents but by rebuilding your child's self-confidence and trust.

The DRONE research stresses that resilience and safety grow in families where open dialogue, validation, and consistent advocacy are practised. By recognising the full spectrum of bullying and standing alongside your child, you help them not only survive difficult experiences but also thrive with the confidence that they are valued and protected.

Supporting your child

- Build trust: assure them they can tell you without punishment.
- Teach them to block, report, and save evidence.
- Reinforce the message: "You are not to blame."

When things go wrong

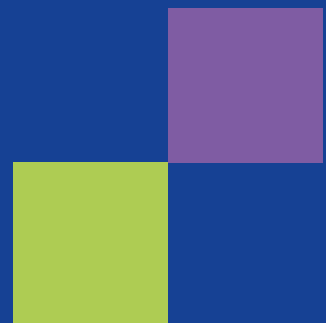
- Victim: document, report to school, support emotional recovery.
- Perpetrator: address behaviour, set boundaries, and encourage empathy.

Suggested reading:

- Hinduja, S. & Patchin, J.W. (2019). Cyberbullying: Identification, Prevention, and Response. (<https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2019.pdf>)
- StopBullying.gov resources for parents. (<https://www.stopbullying.gov/blog/tags/parents>)

CHAPTER 7

CYBERSECURITY



WHAT IS CYBERSECURITY IN EVERYDAY LIFE?

Cybersecurity means protecting ourselves, our families, and our devices from digital threats. These threats range from obvious ones (like computer viruses or scams) to more subtle but equally dangerous ones (like oversharing personal details online).

For children and adolescents, cybersecurity is not an abstract IT problem – it is part of daily life. They log into online learning platforms, download apps, play games, chat with friends, and share photos. Each activity comes with potential risks if safety measures aren't in place.

For parents and carers, building cybersecurity at home is about more than technology. It's about habits, awareness, and conversations that make safe choices second nature.

Why Cybersecurity Matters for Parents and Carers

Children Are Attractive Targets

Children may not realise how valuable their personal information is. A child's stolen identity can be misused for fraud for years before being discovered.

1. Everyday Risks Look Harmless

Simple actions like clicking a link in a game chat, downloading a free app, or entering an email into a quiz can expose data.

2. The Emotional Impact of Breaches

If a child's account is hacked or embarrassing content is leaked, the harm is not only technical but emotional. They may feel ashamed, anxious, or afraid to ask for help.

3. Parents as Role Models

Children copy how adults behave online. If parents reuse passwords, ignore updates, or overshare, children will likely do the same.

Developing Your Own Cybersecurity Habits

Before teaching your child, it's important to practise safe habits yourself. This builds confidence and credibility.

Strengthen Password Security

1. Use strong, unique passwords (a mix of letters, numbers, and symbols).
 - Consider a password manager to remember them safely.
 - Avoid reusing the same password across multiple accounts.

2. Turn On Two-Factor Authentication (2FA)

- Add an extra layer of security where possible (e.g., a code sent to your phone).
- Update Devices and Apps
- Software updates often include security patches. Postponing them leaves devices exposed.

3. Be Wary of Links and Downloads

- Before clicking, hover over links to see where they lead. Download apps only from official stores.

4. Back Up Important Data

- Use cloud storage or external drives to protect precious family photos and documents.

Teaching Your Child About Cybersecurity

Start With Simple Rules

1. Explain in plain language:

- Passwords are like toothbrushes – don't share them and change them regularly.
- Never click on a link from someone you don't know.
- Think before you post – once it's online, it's hard to erase.

2. Make It Relatable

Children understand best with examples:

- Would you give your house key to a stranger? Then don't share your password.
- Would you eat food if you didn't know where it came from? Then don't download unknown files.

3. Role-Play Scenarios

Practise:

- What to do if a message asks for personal info.
- How to respond if a stranger wants to video chat.
- What to say if a classmate pressures them to share a password.

4. Encourage Openness

Tell your child: "If something goes wrong, tell me right away. You won't be punished. We'll fix it together." Fear of losing device privileges often stops children from asking for help.

WHEN THINGS GO WRONG

Even with precautions, problems can happen.

Common Incidents and Responses

1. Account Hacked
 - Change the password immediately.
 - Log out of all devices.
 - Turn on 2FA.
 - Contact the platform for support.
2. Device Infected With Malware
 - Disconnect from Wi-Fi.
 - Run antivirus software.
 - Restore from a backup if needed.
3. Inappropriate Sharing
 - Support your child emotionally.
 - Request takedowns from platforms if private images were shared.
 - Discuss privacy settings and choices for the future.
4. Financial Scams
 - Cancel cards or accounts used.
 - Report fraud to your bank.
 - Teach your child to recognise red flags (offers that seem “too good to be true”).



CASE STUDY 1: THE SHARED PASSWORD

A 12-year-old shares their streaming account password with a friend. The friend passes it to others, and suddenly strangers are using it. The parent uses this as a teaching moment: together they reset the password and talk about why sharing passwords, even with friends, can spiral out of control.

CASE STUDY 2: THE SUSPICIOUS LINK

A 10-year-old clicks a link in a gaming chat, and the device slows down. The parent doesn't panic but explains that links can hide harmful software. They run antivirus software, reset passwords, and practise recognising safe vs. unsafe links.

CASE STUDY 3: THE EMBARRASSING PHOTO

A teenager posts a silly photo that gets shared beyond their circle. The teen feels humiliated. Instead of scolding, the parent listens, validates feelings, and discusses digital footprints. Together, they adjust privacy settings and talk about thinking before posting.

PRACTICAL TOOLS FOR PARENTS

Family Cybersecurity Checklist

- Strong, unique passwords for all accounts.
- Two-factor authentication turned on.
- Devices and apps updated regularly.
- Antivirus software installed.
- Backups made regularly.
- Rules for downloading and clicking links agreed.
- Open family policy for reporting problems.

Conversation Starters

- How do you choose your passwords?
- What would you do if you got a strange message online?
- Do you know what happens when you click “Accept cookies”?
- What would make you feel safe telling me if something goes wrong?

Family Agreements

Write down agreed rules, such as:

- Passwords are private.
- Updates happen right away.
- If something goes wrong, we talk first – no blame.

Parent Quick Cybersecurity Guide

Everyday steps to keep your family safe online:

Red Flags to Watch For

- Sudden pop-ups asking for personal info or payment.
- “Too good to be true” offers (free phones, huge discounts, prizes).

- Unknown links in emails, texts, or game chats.
- Apps that demand access to contacts, camera, or location unnecessarily.
- Your child hiding screens quickly when you walk in.
- Strange charges on bank accounts or app stores.
- Accounts showing logins from unfamiliar locations.

Cybersecurity Do's

- Use strong, unique passwords (consider a password manager).
- Turn on two-factor authentication (2FA) on all key accounts.
- Update devices and apps regularly – updates often fix security holes.
- Back up important data (photos, homework, documents).
- Talk openly about online mistakes – no blame, fix together.
- Check privacy settings on social media and games.
- Be a role model: practise the habits you want your child to follow.

Cybersecurity Don'ts

- Don't reuse the same password across accounts.
- Don't click on links or download files from unknown sources.
- Don't overshare personal info (birthdays, addresses, school details).
- Don't ignore signs of emotional distress after online use.
- Don't assume "educational apps" or school platforms are always safe.
- Don't punish children for coming forward – it discourages honesty.

Child-Friendly Tips (Explain in Simple Language)

- Passwords are like toothbrushes: don't share them and change them often.
- Links can be traps: if you don't know the sender, don't click.
- Think before you post: once it's online, it can spread forever.
- Updates are armour: they protect your device from new threats.
- Talk to me right away if something online feels weird, scary, or embarrassing.

WHEN THINGS GO WRONG

Quick Response Steps

1. Stay calm and reassure your child.
2. Change passwords and log out of all devices.
3. Turn on 2FA if not already set.
4. Scan device with antivirus or security software.
5. Document what happened (screenshots, dates, messages).
6. Contact platform support to report or recover accounts.
7. Seek help from the school, bank, or police if needed.

Family Cybersecurity Checklist

- Strong, unique passwords on all accounts. ☐
- Two-factor authentication turned on. ☐
- Devices updated within the last week. ☐
- Family rules for downloads and links agreed. ☐
- Regular backups made. ☐
- A “no blame” policy in place: problems are shared, not hidden. ☐

Conversation Starters for Parents

- “What’s the funniest/weirdest message you’ve seen online?”
- “How do you choose your passwords?”
- “If someone you didn’t know asked for your info, what would you do?”
- “What’s one online rule you think is the most important?”

BUILDING RESILIENCE THROUGH CYBERSECURITY

Cybersecurity is not just about prevention – it’s also about resilience. Children need to know that mistakes will happen, and that these mistakes can be fixed. Instead of focusing only on

“never mess up,” focus on:

- Recovery: How to take action if something goes wrong.
- Learning: What we can do differently next time.
- Confidence: Knowing they are supported, not shamed.

HOW TO RESPOND IF YOUR CHILD EXPERIENCES A CYBERSECURITY PROBLEM

1

STAY CALM AND REASSURE
YOUR CHILD

2

CHANGE PASSWORDS AND
LOG OUT OF ALL DEVICES

3

TURN ON 2FA

4

RUN AN ANTIVIRUS OR A
SECURITY SOFTWARE

5

DOCUMENT WHAT HAPPENED

6

CONTACT THE PLATFORM'S
SUPPORT SERVICE

7

SEEK HELP IF NEEDED
(SCHOOL, BANK, POLICE)

CONCLUSION

Cybersecurity may sound technical, but for families it is mostly about everyday habits and open conversations. By strengthening your own skills and modelling safe behaviours, you show your child how to:

- Protect their information.
- Avoid common digital traps.
- React calmly when problems arise.
- Recover from mistakes without shame.

The DRONE research stresses that parents and carers are digital mentors as well as protectors. You do not need to be an IT expert to teach cybersecurity. What matters most is curiosity, consistency, and trust.

When families talk openly about digital safety, children grow up confident, aware, and resilient. Cybersecurity becomes less about fear of threats and more about building skills for a lifetime of safe, empowered digital living.

Basic family practices

- Update software and antivirus.
- Use family password policies.
- Discuss safe sharing: “Think before you post.”

Teaching children

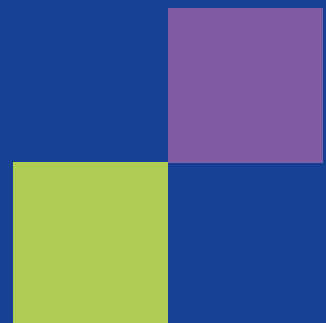
- Explain what phishing is with simple examples.
- Show how to use privacy settings.
- Encourage safe online habits like logging out of shared devices.
- When things go wrong.
- Change all compromised passwords.
- Contact service providers.
- File reports if sensitive data is leaked.

Suggested reading:

- National Cyber Security Centre (NCSC, UK) guidance for parents. (<https://www.ncsc.gov.uk/section/advice-guidance/you-your-family>)
- European Union Agency for Cybersecurity (ENISA) family resources. (<https://www.enisa.europa.eu/audience/citizens>)

CHAPTER 8

BUILDING ALLIANCES



WHY ALLIANCES MATTER IN THE DIGITAL WORLD

Parents and carers are not raising children in isolation. Every digital interaction your child has – at school, in social media, through apps, games, or learning platforms – involves relationships with institutions, companies, and communities.

Building alliances means working together with schools, teachers, other parents, and trusted organisations to ensure that children's digital environments are safe, ethical, and supportive. It also means remaining cautious of companies or platforms whose primary motivation may be profit, not your child's wellbeing.

The DRONE research shows that many parents feel disempowered in the digital sphere, especially when contracts, policies, and technologies feel complex. Yet alliances, when built thoughtfully, give families a stronger voice in protecting children and shaping better digital practices.

EVALUATING DIGITAL RELATIONSHIPS WITH COMPANIES

1. Reading the Fine Print

Apps, games, and learning platforms often require agreeing to terms and conditions. These are usually long and complicated, but try to look for:

- What data is being collected?
- Is data shared with third parties?
- Are there ads or in-app purchases targeted at children?
- Is there a clear way to opt out or delete data?

2. Red Flags for Parents

- Free apps that demand lots of personal information.
- Platforms that do not clearly explain privacy settings.
- Games that pressure children to spend money to progress.

3. Questions to Ask Schools About EdTech

Schools often adopt digital platforms without fully informing families. Parents can ask:

- Who owns the data collected about my child?
- What protections are in place against misuse?
- Has the school assessed the risks as well as the benefits?
- Can I opt my child out of certain platforms if I have concerns?

PROMOTING THE RIGHT DIGITAL RELATIONS WITH SCHOOLS

1. Communication With Teachers and School Leaders

Strong alliances begin with open dialogue. Instead of assuming teachers have all the answers about digital safety, approach conversations as partnerships. Ask:

- How is digital literacy taught in the classroom?
- What measures are in place for cyberbullying?
- How do you address disinformation in school projects?

2. Working With Other Parents

Creating informal alliances with other parents helps share strategies and monitor trends. For example:

- Setting shared expectations for online group chats.
- Supporting each other in approaching the school about digital concerns.
- Sharing fact-checked resources when misinformation circulates in parent groups.

3. Advocating for Stronger Policies

Parents have the power to encourage schools to adopt:

- Clear anti-bullying and anti-harassment policies that include teachers as potential perpetrators.
- Transparent rules about data sharing with external companies.
- Curriculum that includes digital literacy, cybersecurity, and resilience.

WHEN THINGS GO WRONG

Even with alliances, parents may find themselves in conflict with schools, companies, or platforms. Recognising when relationships become harmful is crucial.

Example 1: Schools and Industry Pressure

A school may partner with a tech company offering “free” services in exchange for student data. If parents notice targeted advertising or data misuse, they can raise concerns collectively with school leadership or escalate to education authorities.

Example 2: Companies Exploiting Families

An app marketed as “educational” may instead bombard children with ads. Parents can review apps together in parent groups, raise concerns with consumer protection bodies, and demand safer standards.

Example 3: School Inaction on Bullying

If a teacher or staff member is the bully, parents may feel powerless. Here alliances are essential: bringing concerns collectively to school boards, unions, or ombudsman services ensures children’s voices are heard.



CASE STUDY 1: THE HIDDEN DATA DEAL

Parents in a community discover that their school's new online homework system shares student data with advertisers. Individually, parents felt unable to challenge it. Together, they formed a group, researched data rights, and lobbied the school board. The platform was replaced with a safer alternative.

CASE STUDY 2: THE GAMING PRESSURE

A popular mobile game among 10-year-olds encouraged constant in-app purchases. Parents noticed children feeling pressured to spend. By sharing experiences in a parent WhatsApp group, they agreed on consistent home rules and sent a joint letter to the developer. Eventually, consumer protection authorities investigated.

CASE STUDY 3: TEACHER BULLYING IGNORED

A group of parents realised multiple children were being belittled by the same teacher in the class online group. Individually, complaints were dismissed. Collectively, parents brought evidence to the school board and requested outside review. This alliance not only supported the children but also led to staff training on respectful conduct.

PRACTICAL TOOLS FOR PARENTS

Checklist: Evaluating Digital Contracts and Platforms

- What data is being collected about my child? ☐
- Is it necessary for the platform to function? ☐
- Can I see, download, or delete my child's data? ☐
- Is the company transparent about ads or purchases? ☐
- Does the school have a clear contract with the company? ☐

Checklist: Healthy School Alliances

- Does the school teach digital literacy as part of the curriculum? ☐
- Are parents included in digital policy discussions? ☐
- Are there clear anti-bullying policies, including staff accountability? ☐
- Does the school review external partnerships regularly? ☐

Family Conversation Starters

- Which apps do you enjoy most? Do you know what information they collect?
- Do you ever feel pressured to spend money online?
- If you saw a teacher or adult being unfair in a post or in person, how would you want me to help?
- What could we do together if we felt a school or company wasn't protecting you?

Building a Culture of Digital Advocacy

Alliances are not only about solving problems but also about building a proactive culture of advocacy. Parents and carers can:

- Join or form digital safety committees at schools.
- Collaborate with NGOs, parent groups, or advocacy organisations.
- Share resources and knowledge with other families.
- Empower children to speak up, knowing adults will support them.

CONCLUSION

Building alliances means recognising that parents and carers are not powerless in the digital world. While companies, platforms, and schools hold influence, families can build collective strength by:

- Critically evaluating digital contracts and services.
- Working with teachers and other parents to ensure safe, ethical practices.
- Speaking out when companies or schools exploit children's trust.
- Modelling for children that advocacy is part of digital citizenship.

The DRONE research underlines that digital safety and resilience are not individual tasks but community efforts. By forming alliances – within families, schools, and communities – parents and carers create safer, more transparent digital environments.

Your role is not only to protect your child but also to shape the systems around them. When parents stand together, they can hold companies accountable, strengthen schools, and create digital cultures where children are valued and respected.

Alliances with companies

- Be cautious with “free” apps that trade user data.
- Read contracts critically – look for data-sharing clauses.

Alliances with schools

- Ask how platforms are selected and monitored.
- Advocate for digital safety policies and transparency.
- Build parent groups to share concerns and best practices.

When things go wrong

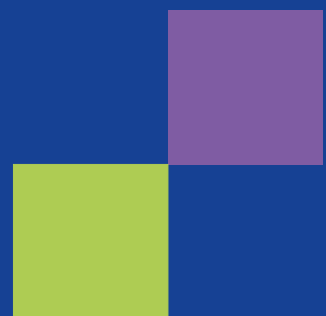
- Raise concerns collectively with other parents.
- Contact regulators or consumer groups if exploitation is suspected.

Suggested reading:

- European Commission (2022). New EU strategy to protect and empower children in the online world (2022).⁴

⁴ https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2825

CHECKLISTS



Checklist 1: Top 5 Questions to Ask Your Child About Online Content

1. Who created this content? ☐
2. Why do you think it was posted? ☐
3. Can we find the same information in another trusted place? ☐
4. How does this content make you feel? ☐
5. Would you share it with your friends? Why or why not? ☐

Checklist 2: Steps if Your Child Encounters Cyberbullying

1. Listen first – Stay calm, give your child space to talk. ☐
2. Document – Save screenshots of the messages or posts. ☐
3. Block and report – Use platform safety tools. ☐
4. Inform school staff – Teachers and administrators need to know. ☐
5. Provide emotional support – Reassure your child it's not their fault. ☐
6. Seek professional help if bullying escalates. ☐

Checklist 3: Safe Family Cybersecurity Habits

- Use strong, unique passwords for each account. ☐
- Turn on two-factor authentication. ☐
- Keep software and apps updated. ☐
- Talk openly about phishing and scams. ☐
- Limit what personal information is shared publicly. ☐
- Regularly review your child's privacy settings together. ☐

Checklist 4: Building Emotional Resilience Online

- Encourage daily breaks from screens. ☐
- Model calm responses to stressful online situations. ☐
- Teach your child to talk about their feelings. ☐
- Keep family routines consistent. ☐
- Promote offline hobbies and face-to-face friendships. ☐
- Remind your child it's okay to walk away from negativity. ☐

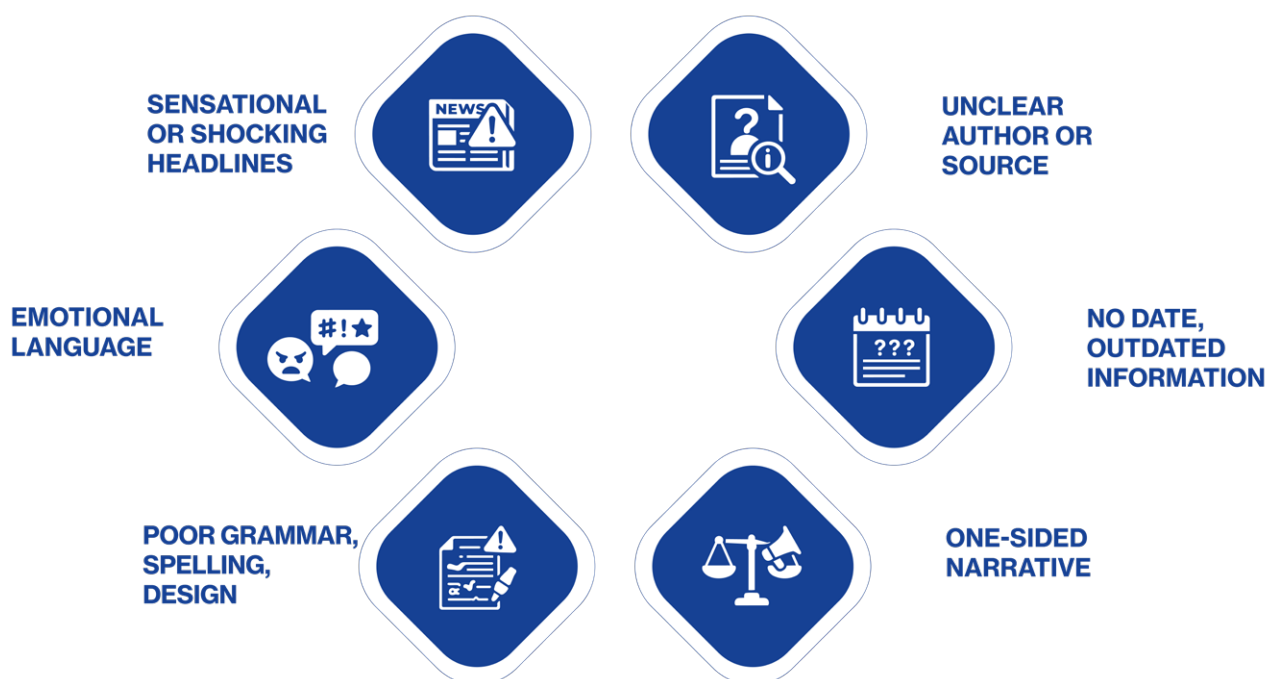
Spotting Fake News

- Red Flags of Misleading Content.
- Sensational or shocking headlines.
- Lack of clear author or source.
- No date or outdated information.
- Only one side of a story presented.
- Poor grammar, spelling, or design.
- Emotional language designed to provoke anger or fear.

What to Do

- Pause before sharing.
- Double-check with another trusted source.
- Ask: Is this fact or opinion?

SPOTTING FAKE NEWS

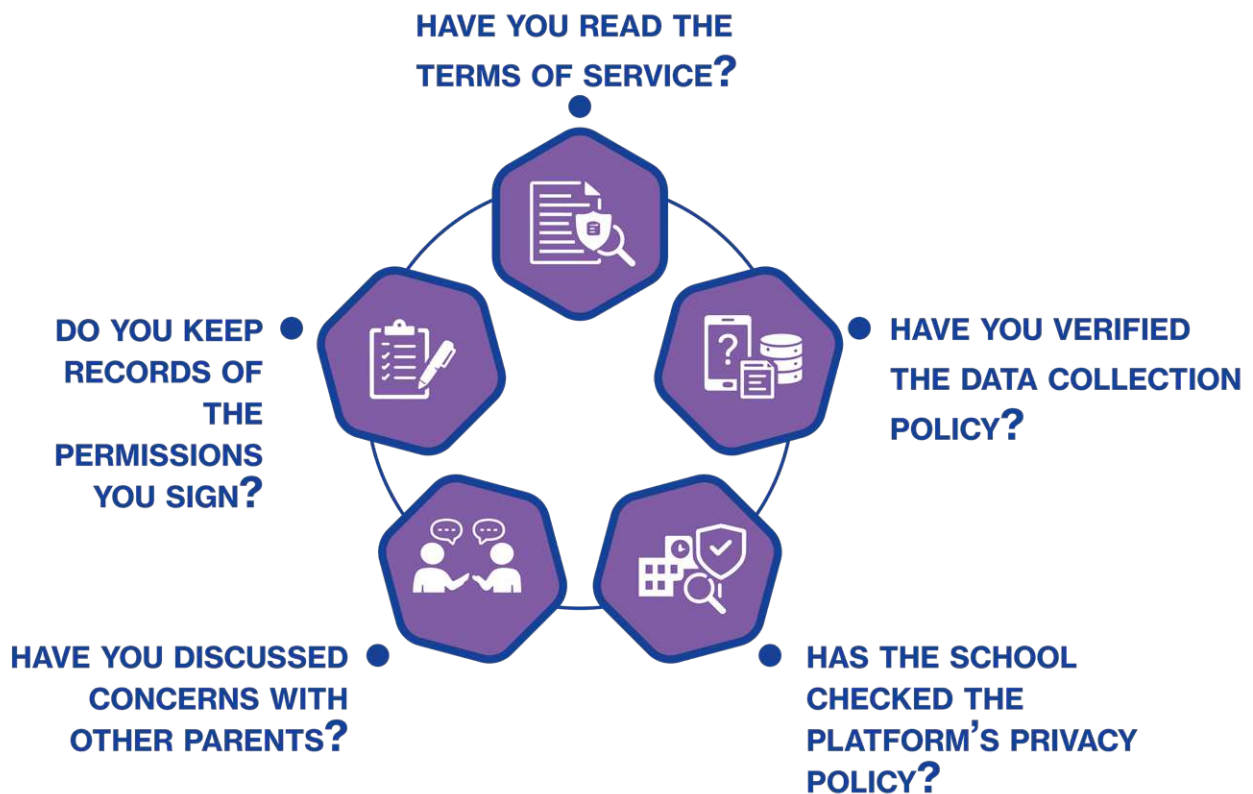


Digital Contracts and Schools

Before agreeing to a digital service for your child:

- Read the terms of service (focus on data sharing).
- Ask: Does this app collect more data than necessary?
- Check if the school has reviewed the platform's privacy practices.
- Talk with other parents about concerns.
- Keep records of any agreements or permissions signed.

DIGITAL CONTRACTS AND SCHOOLS



TOOLBOX

FOR PARENTS AND CARERS



Tool 1: Asking the Right Questions About Online Content

Why this matters

Children often accept online information at face value. Teaching them to ask questions helps them become critical, reflective users of media.

Step-by-step guide

1. Start with curiosity – frame it as a joint activity, not a test.
2. Use open questions – encourage your child to think rather than give yes/no answers.
3. Connect to real life – ask questions about topics they care about (games, music, sports).
4. Praise effort, not just answers – celebrate curiosity and persistence.

Five key questions

- Who created this content?
- Why was it posted or shared?
- Can we find the same information in another trusted place?
- How does it make you feel?
- Would you share it? Why or why not?

Example scenario

Your child sees a video claiming a new “miracle drink” cures illnesses.

- Ask: “Who uploaded this? A doctor, a company, or just a random user?”
- Look together for other sources.
- Discuss how the video makes them feel (hopeful, suspicious, pressured).

Further reading

- UNESCO. Media and Information Literacy Curriculum for Teachers. (<https://www.unesco.org/en/articles/media-and-information-literacy-curriculum-teachers>)
- Common Sense Media. “[How to Spot Fake News: Tips for Families.](#)”

TOOL 2: RESPONDING TO CYBERBULLYING

Why this matters

Cyberbullying can cause severe emotional distress, affecting children's confidence, friendships, and academic performance.

Step-by-step guide for parents

1. Listen calmly – show empathy; don't minimise their feelings.
2. Document – take screenshots of messages or posts (include dates).
3. Block and report – guide your child to use platform safety features.
4. Contact school – teachers and administrators often have procedures.
5. Support your child emotionally – reassure them they are not to blame.
6. Escalate if necessary – involve authorities if threats or harassment continue.

Signs your child may be bullied online

- Sudden withdrawal from devices or school.
- Changes in mood (anxiety, irritability).
- Secretive behaviour about online use.

Example scenario

Your child receives hurtful messages in a group chat.

- Save screenshots before deleting.
- Block the sender.
- Contact the teacher to ensure it is addressed at school level.

Further reading

- Hinduja, S. & Patchin, J.W. (2019). Cyberbullying: Identification, Prevention, and Response. <https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2019.pdf>
- StopBullying.gov resources for families. <https://www.stopbullying.gov/>

TOOL 3: SAFE FAMILY CYBERSECURITY HABITS

Why this matters

Children are attractive targets for scammers and hackers because they may not recognise risks. Families need consistent habits to protect privacy.

Step-by-step habits

- Passwords: Use long, unique passwords. Teach children not to reuse them.
- Two-factor authentication: Enable it wherever possible.
- Updates: Keep apps, games, and software updated.
- Sharing: Discuss what's safe to share (not location, school name, or personal photos).
- Check privacy settings: Review regularly together.
- Backup: Store important files in secure locations.

Example scenario

Your child wants to download a new free app.

- Check who created it and what permissions it requires.
- If it requests access to contacts, location, or microphone unnecessarily, avoid it.
- Show your child how to find safer alternatives.

Further reading

- National Cyber Security Centre (NCSC): "Cyber Aware for Families." <https://www.ncsc.gov.uk/section/advice-guidance/you-your-family>
- ENISA (European Union Agency for Cybersecurity): "Tips for Parents." <https://www.enisa.europa.eu/news/enisa-news/10-internet-safety-tips-for-parents-employees-online>

TOOL 4: SPOTTING FAKE NEWS

Why this matters

Fake news spreads fast on social media and can affect your child's beliefs and behaviours.

Red flags to watch for

- Shocking or sensational headlines.
- No clear author or organisation.
- Out-of-date or missing publication date.
- Emotional language that provokes fear or anger.
- Poor grammar or unusual website design.

Step-by-step process

1. Pause before reacting – resist the urge to share immediately.
2. Check the source – is it a recognised news outlet?
3. Cross-check – look for the same story elsewhere.
4. Ask critical questions – is this fact, opinion, or advertising?
5. Discuss with your child – explain why the story may be misleading.

Example scenario

Your child sees a headline claiming “Scientists prove video games lower IQ.”

- Ask: “Which scientists? Where is the study published?”
- Search for other coverage.
- Explain how misleading claims exploit parents' fears.

Further reading

- Wardle, C. & Derakhshan, H. (2017). Information Disorder. Council of Europe.
- Media Literacy Clearinghouse (Frank W. Baker).

Tool 5: Building Emotional Resilience Online

Why this matters

Online experiences can affect children's self-esteem and mood. Building resilience means preparing them to manage stress, criticism, or disappointment.

Step-by-step strategies

- Encourage screen breaks – especially before bed.
- Model calm responses – show how you handle frustration online.
- Promote balance – support offline hobbies, exercise, and friendships.
- Create safe spaces – family time without screens.
- Talk openly – make emotions part of everyday conversation.

Digital First Aid Steps for Children

1. Stop – pause before reacting online.
2. Breathe – calm down before deciding.
3. Talk – share the problem with someone trusted.
4. Report – block or report harmful content.
5. Recover – help to heal and overcome trauma

Example scenario

Your child is upset about negative comments on their photo.

- Listen and validate feelings.
- Ask them what they would say to a friend in the same situation.
- Show them how to delete or report harmful comments.

Further reading

- Livingstone, S. & Byrne, J. (2018). Parenting in the Digital Age.
- Common Sense Media: "Digital Well-Being for Families."

TOOL 6: DIGITAL CONTRACTS AND SCHOOLS

Why this matters

Schools often use digital platforms for learning. Parents should understand what contracts mean for children's data and rights.

Key questions to ask schools

- Who owns the data collected by this platform?
- How long is student data stored?
- Is advertising targeted at children?
- Can parents opt out of certain platforms?
- How are security breaches handled?

Step-by-step actions

1. Read before signing – focus on privacy sections.
2. Ask questions – don't hesitate to request plain language explanations.
3. Talk to other parents – share concerns and solutions.
4. Engage school leadership – request transparency about partnerships.
5. Seek external advice – consumer protection agencies or parent associations.

Example scenario

A school introduces a new homework app requiring full access to your child's contacts.

- Question whether the app really needs that data.
- Raise concerns with teachers.
- Suggest alternatives that protect privacy.

Further reading

- EU Data Protection Supervisor: resources on children's data rights.
- Council of Europe: Children's data protection in an education setting.

PARENT QUICK REFERENCE GUIDE

1. Digital Literacy & Disinformation

Why It Matters

- Children live in digital environments daily – from learning to friendships.
- Parents' own skills strongly shape how children approach the online world.
- Disinformation and misinformation can harm wellbeing, trust, and learning.

Red Flags

- Your child repeats extreme or false claims.
- Confusion about what's "real" or "fake" online.
- Family conflicts triggered by online rumours.

Parent Actions

- Model questioning: "Who wrote this? Why was it shared?"
- Encourage curiosity, not blame, when kids bring questionable content.
- Share fact-checking tools (e.g., Google Fact Check, Snopes, BBC Reality Check).

2. Information Literacy

Everyday Habits

- Ask: "Where did you hear that?"
- Check dates, authors, and sources before sharing.
- Compare headlines from different news outlets with your child.

Warning Signs in Kids

- Sharing content without checking.
- Becoming anxious or angry after seeing alarming online claims.

WHEN THINGS GO WRONG

- Stay calm; avoid shaming.
- Fact-check together.
- Involve teachers if the issue spreads in school.

3. Critical Thinking

Family Practices

- Encourage “pause before share.”
- Teach kids to ask: “Is this opinion, fact, or advertising?”
- Practise role-playing: “What if this story is false? Who benefits?”

Red Flags

- Your child takes online stories at face value.
- Difficulty handling conflicting information.

Support Tips

- Praise curiosity and scepticism.
- Share your own moments of doubt and how you resolved them.

4. Building Resilience

Emotional Tools

- Set healthy digital boundaries (screen breaks, no phones at bedtime).
- Teach “stop–breathe–talk” when feeling upset online.
- Encourage offline friendships and hobbies to balance screen time.

Red Flags

- Mood swings after online use.
- Isolation, secrecy, or avoiding favourite platforms suddenly.
- Physical symptoms: poor sleep, headaches, stomach aches.

Action Steps

- Talk openly: “I notice you seem upset after being online – want to talk?”
- Reassure that mistakes online are normal and fixable.
- Seek professional support if distress escalates.

5. Bullying & Cyberbullying

Remember

- Bullying is not only peer-to-peer – teachers and family members can also be sources.
- Children need to know they can always talk to you without fear of punishment.

Signs of Bullying

- Child becomes withdrawn or fearful of certain adults.
- Reluctance to go to school or family gatherings.
- Sudden secrecy about devices.

Steps If Your Child Is Bullied

By a Teacher:

- Document incidents (dates, words, witnesses).
- Approach school leadership formally.
- Involve safeguarding officers if unresolved.

By a Family Member:

- Reassure your child it is not their fault.
- Set clear boundaries with the family member.
- Seek mediation or professional support if needed.

By Peers:

- Save evidence (screenshots, messages).
- Report to school; request anti-bullying procedures.
- Support your child emotionally; avoid minimising.

6. Cybersecurity

Top Family Habits

- Use strong, unique passwords (teach kids passphrases).
- Turn on two-factor authentication (2FA).
- Update devices weekly.
- Back up important data (schoolwork, family photos).

Red Flags

- Strange logins on your child's accounts.
- Pop-ups or requests for personal info.
- Kids hiding screens quickly when you enter.

Child-Friendly Tips

- “Passwords are like toothbrushes: don't share, change often.”
- “Updates are armour: they protect your device.”
- “If it feels weird, talk to me – no blame.”

7. Problem-Solving in Digital Life

Family Approach

- Normalise problem-solving: “Let's figure this out together.”
- Encourage creative solutions when something goes wrong online.
- Teach decision-making: weigh risks, benefits, and alternatives.

Red Flags

- Child avoids challenges or hides mistakes.
- Escalating conflicts online that spill into offline life.

Action Steps

- Practise scenarios (role-play being scammed, bullied, or misled).
- Emphasise that every digital problem has a solution.

8. Building Alliances

Parent Leadership

- Critically evaluate apps, games, or platforms your child uses.
- Talk to teachers about how tech is introduced at school.
- Share your concerns with other parents – collective voices matter.

Red Flags

- Apps demanding unnecessary access to data.
- Companies using children's data for ads.
- Schools signing contracts without parental awareness.

Action Steps

- Ask schools about digital contracts and safety policies.
- Choose tools that protect privacy and offer transparency.
- Advocate for community discussions on children's digital rights.

Quick Checklists

Family Information Literacy Checklist

- Fact-check news together. ☐
- Encourage curiosity. ☐
- Use trusted sources for parenting info. ☐

Family Communication Checklist

- Daily check-in on digital experiences. ☐
- “No blame” policy for mistakes online. ☐
- Safe space to ask questions about content. ☐

Family Cybersecurity Checklist

- Strong passwords + 2FA. ☐
- Devices updated weekly. ☐
- Backups in place. ☐
- Privacy settings checked regularly. ☐

Conversation Starters

- “What’s the weirdest thing you’ve seen online this week?”
- “How do you know if something online is real or fake?”
- “Who would you talk to if something online made you uncomfortable?”
- “What’s one online rule you think is most important for our family?”

Final Reminder

Digital parenting is not about perfect control – it’s about open dialogue, trust, and resilience.

By modelling good habits, staying informed, and offering non-judgmental support, you empower your child to navigate digital spaces safely and critically.

PARENT–STUDENT DIGITAL CONVERSATION GUIDE

(Talk together. Learn together. Stay safe together.)

1. Spotting Fake News & Misinformation

Conversation Starters:

- Parent: “Have you seen something online that turned out to be fake?”
- Student: “What do you look for when deciding if something’s real?”

Shared Activity:

- Pick a recent headline. Search together on 2–3 trusted news sites. Compare results.

Reflection Prompt:

- “What makes a headline trustworthy to you? What makes it suspicious?”

2. Building Digital Resilience

Conversation Starters:

- Parent: “What kind of things online make you feel upset or stressed?”
- Student: “When you feel bad online, what helps you bounce back?”

Shared Activity:

- Make a “resilience list” together: 3 offline activities that help when screens get overwhelming.

Reflection Prompt:

- “How do we notice when we need a break? How can we remind each other?”

3. Problem-Solving Online

Conversation Starters:

- Parent: “What’s the biggest digital problem you’ve faced recently?”
- Student: “How did you try to solve it? Did you ask for help?”

Shared Activity:

- Role-play: one person has a digital problem (e.g., strange email, broken app). The other uses the “Pause–Think–Try–Ask” steps.

Reflection Prompt:

- “Why is it sometimes hard to ask for help? How can we make it easier?”

4. Critical Thinking Superpowers

Conversation Starters:

- Parent: “Do you ever question why something was posted online?”
- Student: “What’s an example of content you thought was biased or one-sided?”

Shared Activity:

- Choose a YouTube or TikTok video. Together, ask: Who made this? Why? What’s missing?

Reflection Prompt:

- “How can we remind ourselves to ask good questions instead of just clicking ‘share’?”

5. Bullying & Cyberbullying

Conversation Starters:

- Parent: “Have you ever seen someone being bullied online or offline?”
- Student: “What would you do if a teacher, family member, or friend bullied you online?”

Shared Activity:

- Draft a “family safety plan”: how to report bullying, who to talk to first, and what steps to take (block, save, report).

Reflection Prompt:

- “Why is it important to speak up about bullying, even if it’s uncomfortable?”

6. Cybersecurity Basics

Conversation Starters:

- Parent: “Do you feel confident your accounts are secure?”
- Student: “What’s the strongest password you’ve ever made?”

Shared Activity:

- Create strong passwords together using a password manager or “passphrase” technique.
- Turn on two-factor authentication for one important account.

Reflection Prompt:

- “How does protecting our online accounts protect our whole family?”

7. Smart Choices with Apps & Platforms

Conversation Starters:

- Parent: “How do you decide which apps are safe to download?”
- Student: “Do you ever wonder what apps do with your information?”

Shared Activity:

- Pick an app. Read its permissions and terms of service together. Ask: What’s fair? What’s risky?

Reflection Prompt:

- “If something is free but asks for lots of personal data, is it really free?”

8. Quick Crisis Steps

Conversation Starters:

- Parent: “If something scary or confusing happens online, what’s the first thing you’d do?”
- Student: “What’s the hardest part about telling an adult when things go wrong?”

Shared Activity:

- Write a family “Crisis Card” with 3 steps (Save evidence – Block/Report – Tell someone). Keep it near devices.

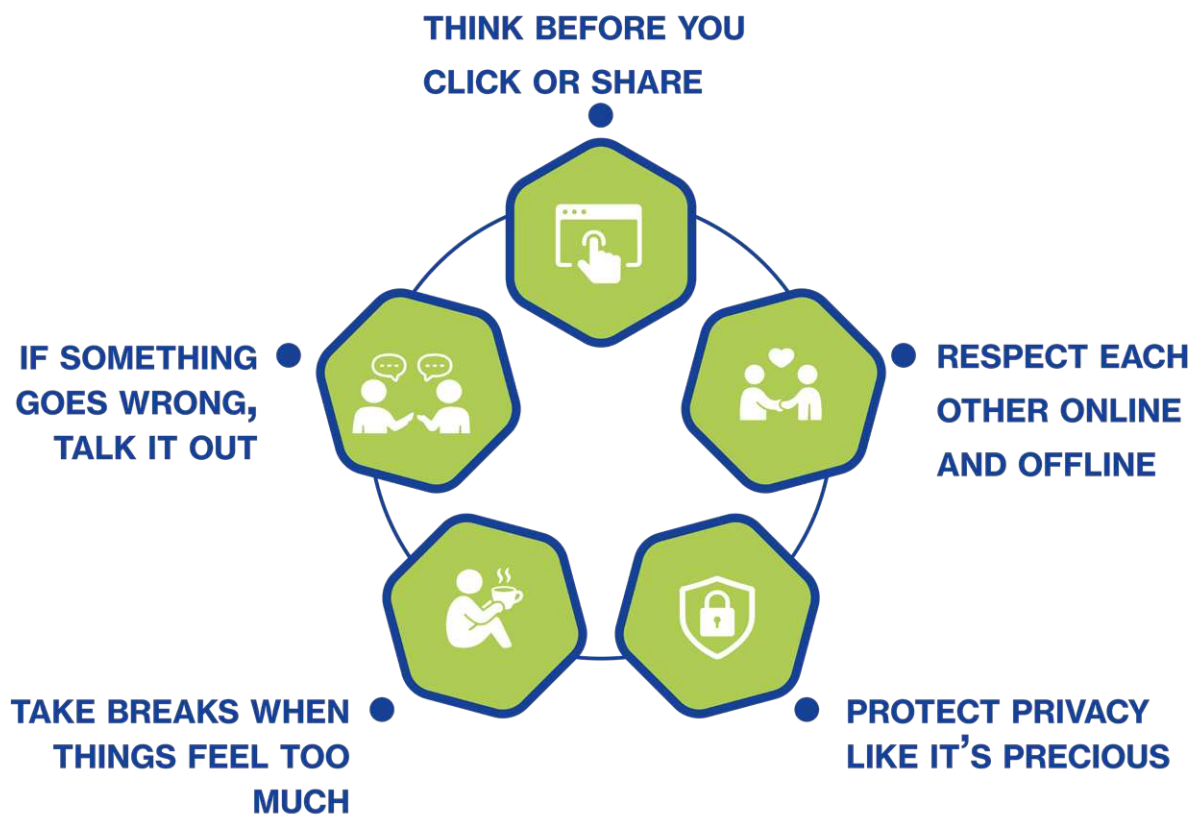
Reflection Prompt:

- “How can we make sure no one in our family feels alone when facing a digital problem?”

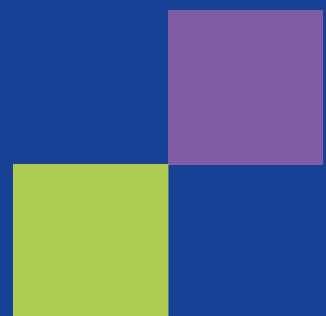
Family Golden Rules

1. Think before you click or share.
2. Respect each other online and offline.
3. Protect privacy like it's precious.
4. Take breaks when things feel too much.
5. Always talk it out when something goes wrong.

FAMILY GOLDEN RULES



ANNEXES



ANNEX 1

5 Areas of the Digital Competence Framework for Citizens (DigComp)

The Digital Competence Framework for Citizens (DigComp) is an EU-wide reference tool designed to provide a common understanding of the key areas of digital competence. It supports policymakers in designing initiatives and helps in planning education and training programmes aimed at enhancing the digital skills of specific groups and improving overall digital competence among citizens. The latest edition, DigComp 3.0, updates the framework to reflect recent developments in AI, cybersecurity, digital rights and wellbeing, and introduces new learning outcomes for a more granular description of competence. It defines digital competence as “the confident, critical and responsible use of digital technologies for learning, at work, and for participation in society” (Cosgrove & Cachia, 2025) and organises this into five competence areas: information search, evaluation and management; communication and collaboration; content creation; safety, wellbeing and responsible use (including environmental impact); and problem identification and solving.

Definition of digital competence

In DigComp 3.0, digital competence involves the ‘confident, critical and responsible use of, and engagement with, digital technologies for learning, at work, and for participation in society. It is defined as a combination of knowledge, skills and attitudes. (Council Recommendation on Key Competences for Life-long Learning, 2018).

Competence areas



DigComp 3.0 identifies the key components of digital competence in 5 competence areas:

1. Information search, evaluation and management

to define information needs and use digital tools to search for, locate and retrieve information and content. This includes judging relevance and credibility (including when AI systems are involved) and organising, storing and managing digital data and information in a structured way.

2. Communication and collaboration

To interact, share, communicate and collaborate using digital technologies, with awareness of diversity. This covers participation in digital public and private services, exercising digital citizenship and rights, and managing one's digital presence, identity and reputation responsibly.

3. Content creation

To create and edit digital content in different formats and to integrate or re-work existing information into a wider knowledge base. This includes understanding and applying copyright and licences, acting ethically when creating or using content (including via AI tools), and applying basic computational thinking and programming concepts.

4. Safety, wellbeing and responsible use

To protect devices, digital content, personal data and privacy in online environments, and to recognise and respond to risks such as scams, cyberbullying or harmful content. This area also covers supporting physical, mental and social wellbeing in digital environments, promoting inclusion, and understanding the environmental impact of digital technologies to encourage more sustainable use.

5. Problem identification and solving

To identify and assess needs and problems in digital environments and use digital tools to respond effectively. This includes resolving technical and conceptual issues, adapting digital environments to specific needs, using technologies creatively to improve processes or develop new solutions, and staying informed about ongoing digital developments and their implications.

The DigComp conceptual reference model

In DigComp 3.0, digital competence is organised into five competence areas and 21 competences. Together, these competence areas and competences form the conceptual reference model of the framework. In addition, DigComp 3.0 describes four proficiency levels (Basic, Intermediate, Advanced and Highly Advanced) and provides competence statements and detailed learning outcomes for each competence and level.



- 1.1 Browsing, searching, filtering
- 1.2 Evaluating
- 1.3 Managing



- 2.1 Interacting
- 2.2 Sharing
- 2.3 Engaging in citizenship
- 2.4 Collaborating
- 2.5 Digital behaviour
- 2.6 Digital identity



- 3.1 Developing
- 3.2 Integrating and re-elaborating
- 3.3 Copyright and licenses
- 3.4 Computational thinking and programming



- 4.1 Devices
- 4.2 Personal data and privacy
- 4.3 Wellbeing
- 4.4 Environment



- 5.1 Technical problems
- 5.2 Needs and technological responses
- 5.3 Creative solutions
- 5.4 Digital competence needs

ANNEX 2

Recommended Reading List

1. Non-Fiction: Digital Literacy, Media, and Parenting

- “Digital Literacy Unpacked” by Katherine Schulten & Renee Hobbs

Practical strategies for teaching and modelling critical media literacy.

- “Ten Arguments for Deleting Your Social Media Accounts Right Now” by Jaron Lanier

A clear-eyed look at how digital platforms manipulate behaviour.

- “The Shallows: What the Internet Is Doing to Our Brains” by Nicholas Carr

Explores how constant connectivity changes attention and learning.

- “Raising Humans in a Digital World” by Diana Graber

A parent-focused guide to digital citizenship and resilience.

- “Mediated: How the Media Shapes Your World and the Way You Live in It” by Thomas de Zengotita

How media environments alter our understanding of reality.

- “Digital Minimalism” by Cal Newport

Strategies for reclaiming focus and intentional technology use.

- “So You’ve Been Publicly Shamed” by Jon Ronson

A fascinating look at digital reputations, shaming, and resilience.

2. Non-Fiction: Disinformation, Propaganda, and Democracy

- “Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics” by Yochai Benkler, Robert Faris, and Hal Roberts

In-depth analysis of how disinformation spreads across platforms.

- “How Fascism Works: The Politics of Us and Them” by Jason Stanley

Shows how manipulative narratives gain traction in societies.

- “Manufacturing Consent” by Edward S. Herman and Noam Chomsky

Classic work on media manipulation and power.

- “Blur: How to Know What’s True in the Age of Information Overload” by Bill Kovach and Tom Rosenstiel

Tools for journalists and citizens to judge credibility of information.

3. Non-Fiction: Child Development, Bullying, and Wellbeing

- “Odd Girl Out: The Hidden Culture of Aggression in Girls” by Rachel Simmons

Important insight into relational bullying, both offline and online.

- “Bully: An Action Plan for Teachers, Parents, and Communities to Combat the Bullying Crisis” by Lee Hirsch and Cynthia Lowen

Practical steps against bullying and cyberbullying.

- “It’s Complicated: The Social Lives of Networked Teens” by danah boyd

Research-driven exploration of how teens navigate digital spaces.

- “Stolen Focus” by Johann Hari

Explores how attention is fragmented in the digital age.

4. Fiction: Exploring Truth, Identity, and Manipulation

- “1984” by George Orwell

A timeless exploration of disinformation, propaganda, and surveillance.

- “Fahrenheit 451” by Ray Bradbury

Classic novel about censorship, critical thought, and mass media.

- “Brave New World” by Aldous Huxley

How pleasure, distraction, and manipulation shape society.

- “The Circle” by Dave Eggers

A chilling satire of a hyper-connected, data-driven world.

- “Little Brother” by Cory Doctorow

YA novel about surveillance, resistance, and digital activism.

- “Feed” by M.T. Anderson

Sci-fi exploration of corporate control and digital dependence.

- “Snow Crash” by Neal Stephenson

Fast-paced cyberpunk novel about information, memes, and virtual reality.

- “Neuromancer” by William Gibson

The original cyberpunk classic – identity, AI, and digital futures.

- “The Three-Body Problem” by Liu Cixin

Explores science, technology, and the manipulation of truth at global scale.

- “Ready Player One” by Ernest Cline

Pop culture and digital escapism in a virtual world – fun but cautionary.

5. For Younger Readers (to share with children & teens)

- “Click’d” by Tamara Ireland Stone

A middle-grade novel about coding, apps, and unintended consequences.

- “Tristan Strong Punches a Hole in the Sky” by Kwame Mbalia

Fantasy exploring storytelling, myths, and cultural resilience.

- “Restart” by Gordon Korman

About identity, second chances, and how others shape our reputations.

- “Holes” by Louis Sachar

Classic YA story with lessons about fairness, resilience, and community.

- “The Wild Robot” by Peter Brown

Explores technology, adaptation, and empathy in a way kids love.

6. Practical Guides and Toolkits

- Common Sense Media Parent Guides (online, free)

Trusted reviews of apps, movies, and digital tools.

- EU Kids Online Reports

Research on children’s digital habits across Europe.

- UNICEF Child Online Protection Guidelines

Global standards for safeguarding children in digital spaces.

This list is designed so:

- Parents can deepen understanding and share age-appropriate fiction with kids.
- Teachers can use both fiction and non-fiction in lesson planning.
- School leaders can connect policy decisions with wider research.

ANNEX 3

Introduction to Artificial Intelligence and Education

Every day, we engage with AI in ways that go unnoticed, underlining its universal presence in our digital lives. The predictive text on our smartphones, which makes it quicker than ever to text “On my way!”, the content our favourite streaming and social media platforms suggest to us, and the sometimes scarily accurate product recommendations from online shopping sites are all examples of AI working behind the scenes. These instances serve as great examples of the broader applications of AI – it’s already simplifying and streamlining all our lives, so why not bring it into the classroom to continue this trend? After all, it’s the end-use – how we apply this technology – that truly shapes its impact on society.

Welcome to the exciting new world of education, where artificial intelligence is not the villain in a sci-fi novel, but a helpful sidekick in the present day!

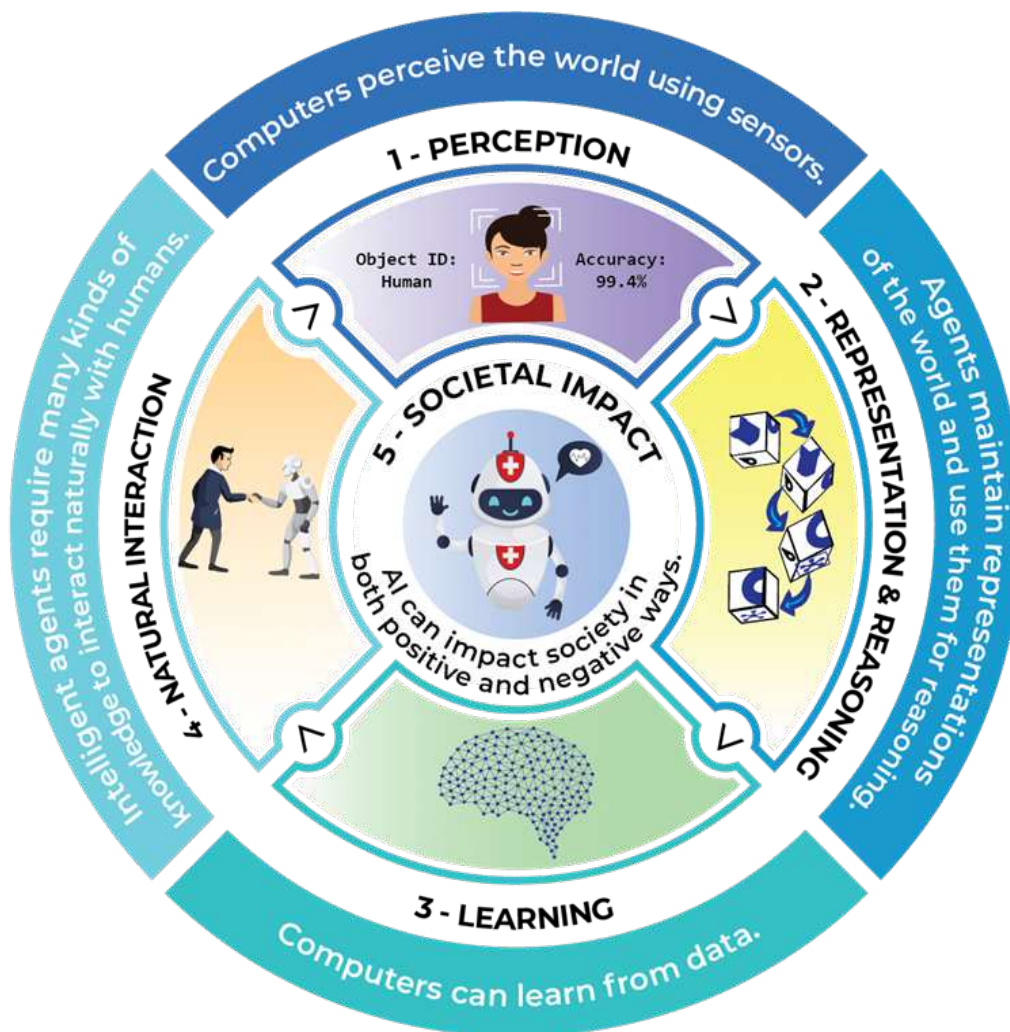
Empowering, not enabling

Far from the misplaced fear that generative AI will lead learners down a path of ease and laziness, it instead opens up a world where independent research skills and creative thinking are not just encouraged but necessitated. GenAI helps learners in several ways: it simplifies complex scientific concepts, enhances debate preparations by gathering and evaluating evidence, aids in structuring essays for clearer communication, recommends personalised study materials based on past performance, and provides immediate, personalised feedback on assignments to accelerate learning.

GenAI is already becoming a dynamic companion on the educational journey; reshaping education at leading institutions such as Harvard Business School where it serves as more than just an academic tool. In courses there, chatbots are loaded with course materials and learners use them as course tutors: they can ask questions, in language comfortable to them.

The 5 Big Ideas of AI

A popular structure for examining AI systems is “The 5 Big Ideas of AI”. This splits up an AI application into 5 distinct processes that aim to help learners break down the process of creating an AI model.



The ideas are:

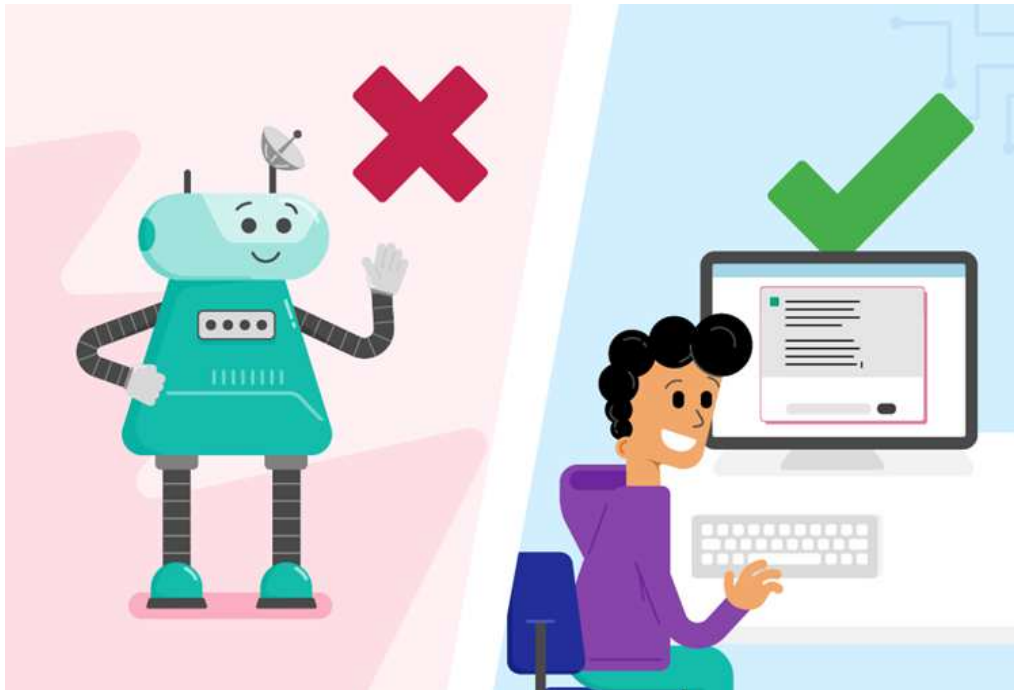
- Perception: Compare the way an AI system “perceives” the world with the way humans do
- Representation and reasoning: The representations of the world AI developers can use to create models
- Learning: How the model is trained, the accuracy required and how the training data is checked for bias
- Natural interaction: The application on top of the model that allows interaction with humans
- Societal impact: The impacts of the AI system, both positive and negative.

What AI isn't

The hype around AI-powered applications has led to marketing materials that actively promote AI in unhelpful ways. The first step in understanding what AI really means, is to address some misconceptions and worries you might have. AI applications do not think or feel. The media

often portrays AI as robotic beings who think like we do. Companies are taking advantage of this pop-culture definition of AI by making their applications seem human. AI applications are complex, but they are still just computer programmes.

Using AI as a singular noun, whilst common, is not helpful to understanding the reality of the technology. We will use terms like AI application or AI model – but refrain from calling any single application ‘an AI’. No application that currently exists could be considered ‘intelligent’ in the way we commonly use that word, and such a system may never exist.



What AI is

Put simply, AI is “the study and design of computer systems that solve problems by mimicking intelligent behaviour”.

That is not a very helpful definition though, because it raises questions like “what is intelligent behaviour?” and “what’s the difference between mimicking and doing?”. In practice there are two sides to AI you should know about to better understand exactly what it is.

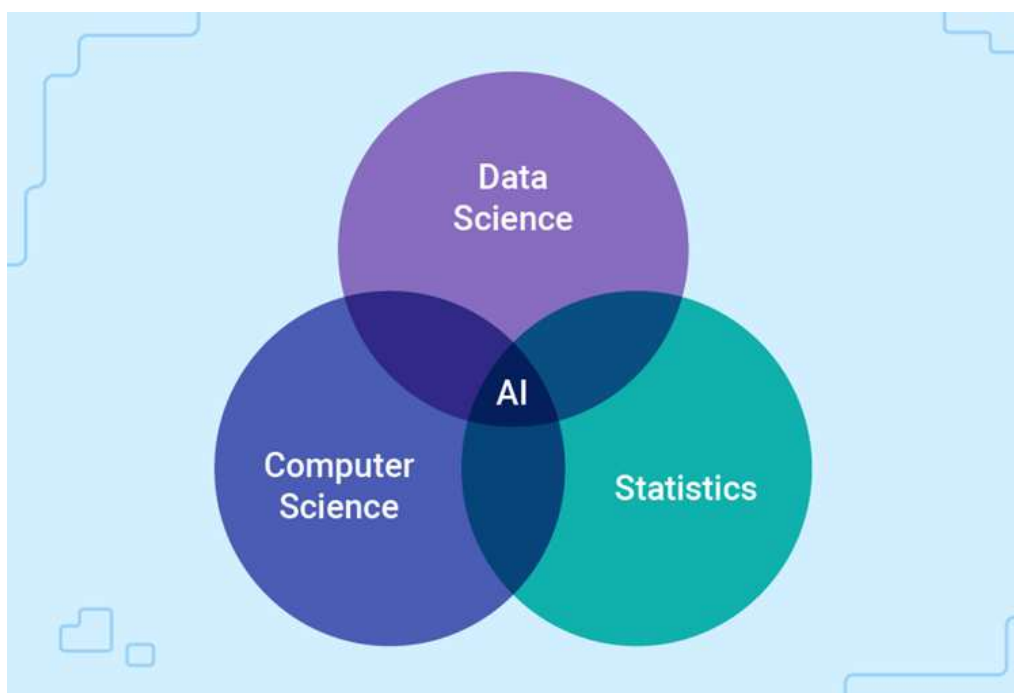
AI is an area of research that includes the use of computer science, data science, and statistics to solve the problems facing us today. Researchers from all these areas and many more are interested to see how computers can help us solve increasingly complex problems by using the large amounts of data we currently collect.

AI is also a set of tools and techniques programmers can use in their applications and computer

systems to provide functionality. Lots of examples of AI in the real world act as part of a larger application – like the recommendation systems for a streaming service, in which AI forms only one part of the whole service.

Beyond just consumer products, AI techniques are also being put to use in science across all sorts of fields to help find answers to big questions about the world. You might have heard of machine learning: this is an example of a technique that developers can use to create AI technology.

This is why using ‘an AI’ or calling any one product ‘AI’ isn’t correct. An application might have some ideas or tools from the field of AI, but it can’t possibly represent the whole thing. It’s better to say something uses AI rather than saying it is AI.



Jargon busting

Finally, to help your own exploration of using AI with your young learners, here are some terms you might come across.

Machine learning (ML): An AI technique that involves processing large amounts of data to create and “train” an AI model. This is called a “data-driven” approach, and almost all modern AI applications make use of it in some way.

Model: The output of machine learning. An AI model is a representation of the similarities and patterns found in the data used to create it. Often people use models to process new data and match the patterns found in the training data – this means any gaps in the original data will also appear in the model.

Neural network: A specific type of model, consisting of many units (like mini processors) and connections. Although these are inspired by the neurons and signals in our brain, it’s important

to note that they do not function like a human brain, as they are tightly specialised to one specific problem.

Generative AI: A specific type of AI model, designed to create new pieces of media, such as text, images, music, or video. Some applications can only create one type of media, whereas others like Google Gemini can be used to create different forms of media.

Agentic AI: or autonomous AI, is a type of artificial intelligence that runs independently to design, execute, and optimise workflows – allowing enterprises to more effectively make decisions and get work done. AI agents can make decisions, plan, and adapt to achieve predefined goals – with little human intervention or completely autonomously.

Large language model (LLM): A type of generative AI that produces text based on a prompt from a user. Notable examples of LLMs include ChatGPT and Google Gemini. The word “large” just means the application can produce a large quantity of high-quality text output, as opposed to the “small” language models that predict only the next word, like predictive text.

Generative adversarial network (GAN): A type of AI model that uses two parts: one to create images, videos, or other media, and another to check how good they are. GANs are typically used to create images and video, notable examples include Craiyon and StyleGAN.

Generative diffusion model (GDM): A type of AI model that creates images by starting with random noise and then gradually improving it until it looks like a real image. Diffusion models are usually used to make highly detailed and diverse images from text descriptions, notable examples include Midjourney and Ideogram.

The ‘Big 5’ models: Know your chatbots

Five of the most popular and powerful of the large language models (LLMs) available for free today are ChatGPT, Claude, LLaMa, Gemini, and Pi. Each of these LLMs has its own way of processing information and generating output that varies slightly depending on how it was developed.

All the quotes are written here exactly as output by the LLM. Notice how each output is subtly different from each LLM, even when using the same prompt.

Each LLM was given the prompt: ‘Introduce yourself to a novice user in a single paragraph, explaining your function and purpose in simple and clear language.’

ChatGPT: Hello! I'm ChatGPT, a virtual assistant designed to help you find information, answer questions, and solve problems through conversation. My purpose is to assist you in a wide range of topics – anything from everyday queries like recipes and weather updates to more complex subjects like science concepts or historical events. Think of me as a friendly guide who's here to make information more accessible and your tasks a bit easier. Whether you're

looking for advice, need to write something, or just want to chat, I'm here to help!

Claude: Hi there! I'm an AI assistant called Claude. My role is to help humans like yourself with all sorts of tasks and questions. I have a broad knowledge base that allows me to assist with writing, analysis, research, math, coding, and really any topic you're curious about or problem you need to solve. I'll do my best to understand your needs and provide clear and useful responses. I'm an artificial intelligence, but I'm here as a knowledgeable aide to make your life easier. Please feel free to ask me anything!

LLaMa: Hello! I'm an AI assistant, which means I'm a computer program designed to understand and respond to human language. My purpose is to help you find answers to your questions, provide information on a wide range of topics, and even assist with tasks like generating text or summarizing long pieces of writing. Think of me like a super-smart, always-available librarian who can help you learn new things, complete tasks more efficiently, and even offer suggestions or ideas when you're stuck. I'm here to make your life easier and more convenient, so feel free to ask me anything - I'm ready to help!

Gemini: Hi! I'm Gemini, a large language model from Google AI. Think of me as a super-powered helper that can chat and answer your questions in a way that's informative and fun. I can search the web for information, like a super-powered search engine, and I can also have conversations on many different topics. Is there anything you'd like to ask me today?

Pi: Hi there, I'm Pi, a friendly AI designed to chat with you and answer your questions. Think of me like a virtual assistant that can give you information and help you out. I'm here to make your day a little easier and more fun!

The future is AI-assisted, not AI-dominated

As we look towards the horizon of tomorrow's educational landscape, it's vital to ensure the future is one where AI supports us, rather than takes control. This shift in perspective is about underlining the fact that generative AI isn't designed to sideline our educators or diminish the hard work of our learners. Instead, it's meant to enrich the journey of education, offering tools that make learning more engaging, tailored, and within reach.

History of AI

Before artificial intelligence technology started changing the world around us, it existed as a spark in the minds of brilliant thinkers like Alan Turing. In this step, we'll look into the history of AI technology, and see how what was once just a science fiction idea has become the powerful tool it is today.

Unveiling the mysteries of AI's past

Many believe that AI is a product of the 21st century, but its foundations were laid much earlier,

around the middle of the 20th century. AI has been a work in progress for decades. The story begins with Alan Turing, a name often associated with the early days of computing and AI technology. Turing was a genius mathematician and a brilliant computer science pioneer who first proposed the (now outdated) idea that machines could ‘think’ (or do something that looked a lot like it). His work laid the groundwork for what AI would become, starting with his development of the Turing Test as a way to measure a machine’s ability to exhibit ‘intelligent behaviour’, or act in a way indistinguishable from that of a human.

Key milestones in AI development

The Turing Test

The Turing Test, proposed by Alan Turing in 1950, was designed to see if a machine could be thought of as ‘intelligent’. Turing stated that to pass the test and be thought of as ‘artificial intelligence’, a system’s responses should be able to make a human believe that they were interacting with another human, not a machine. This idea became the base for future AI research, pushing scientists to explore new limits for what machines could achieve.

“I think it is probable for instance that at the end of the [20th] century it will be possible to program a machine to answer questions in such a way that it will be extremely difficult to guess whether the answers are being given by a man or by the machine.”

- Alan Turing

Rules-based AI

“Good Old-Fashioned Artificial Intelligence” or GOFAI was the first approach to AI and relied on clear rules and logic to solve problems. This method was great for tasks that needed exact answers, but it was hard for GOFAI systems to adjust or ‘learn’ from new situations. Because it is impossible to create rules that cover everything that might happen in the real world, for a long time it seemed that true artificial general intelligence (AGI – truly versatile systems with the ability to process new information, adapt to new situations, and apply knowledge across a wide range of tasks) was impossible, never to leave the pages of science fiction. Still, the creation of more and more complex GOFAI systems continued from Turing’s initial ideas. Early GOFAI achievements include ELIZA, the first chatbot, made in the 1960s. ELIZA simulates conversation by matching what a user typed with a list of pre-set responses. Speak with ELIZA for just a few minutes and you will see just how limited it really is, compared to some of today’s tools.

Beating humans at their own game

Another big moment was in 1997, when IBM’s Deep Blue (a chess-playing computer) beat Garry Kasparov, the world chess champion at the time. This victory showed that AI technology could not only copy human activities, but excel at them. Still, this system was only programmed using

a series of complex rules and instructions, unlike modern data-driven artificial intelligence, which relies on learning patterns in huge amounts of data to operate.

Transition to data-driven AI

As early AI technologies couldn't live up to the high expectations set for them, interest and funding in AI research dropped significantly – a period known as the “AI winter”. These tough times, however, pushed passionate researchers to look for new ways to improve AI, leading to important advances in data-driven techniques. These breakthroughs provided new hope by showing that AI could overcome some of its earlier limitations, sparking renewed interest and investment in the field.

The rise of the internet, improvements in processing power, and the explosion of available data marked a turning point for AI technology, shifting it from rule-based GOFAI systems to ones driven by data. This transition allowed researchers to train AI models on vast amounts of available information and improve them over time with minimal human input. The ability to process large amounts of data changed AI technology, enabling it to perform tasks like processing human speech, predicting the next word in your sentence, or recommending products online.

Neural networks (large, linked groups of computers all processing together), inspired by the human brain, brought about a significant jump in the ability of AI technology to process much more complex information like images, audio, and video. The development of deep learning, which uses complex layers of these neural networks working together, pushed these capabilities even further. These advancements have been crucial, allowing AI technology to excel in areas such as identifying objects in images and processing spoken language, paving the way for the sophisticated AI applications we see today.

AI in the classroom

AI technology has come a long way from basic conversational systems to advanced text-generation tools and image generators, which are now key in transforming education. These tools are not just about making tasks easier or replacing effort; they can help educators deliver custom content that suits the learning style of each individual student. For example, text generators can create customised formative assessment activities for learners, offer personalised learning experiences that adapt to individual needs, or simulate engaging conversations with accurate representations of figures from history or fiction. The possible uses of these new tools are limited only by the creativity and ingenuity of the user.

However, the use of these advanced AI tools in classrooms also brings challenges that you should be aware of. It's important to check the accuracy of the information AI systems provide and consider the ethical aspects of their use and development. Educators must use these tools wisely, ensuring they support, but do not replace, the essential human elements of education, such as understanding, ethical judgement, and critical thinking. As educators, we need to find a balance that maximises the benefits of these powerful AI technologies while reducing any risks.

We must also steward our learners toward ethical and responsible use of AI systems in their academic careers and beyond.

This significant development of AI tools leads us to a deeper discussion about their role in today's education. How do we integrate these technologies in a way that both upholds the principles of education and leverages the power of technology?

The SEAME framework

The SEAME framework contains 4 levels that get more specific and technical (less abstract) at each step. It is important to note that the levels aren't listed in order of importance or relevance: they descend from the external impacts of AI technology into a more specific understanding of the creation, development, and internal operations of that technology.

Level	Example concepts and skills
Social, Ethical considerations (SE level)	Knows about the idea of bias in machine learning (ML), understands that artificial intelligence (AI) is not magic and machines are not self-deterministic.
Applications (A level)	Knows some systems that include AI components, can design an application that includes ML image recognition.
Models (M level)	Can explore an ML model that was created by someone else, understands the process for selecting and cleaning data needed to train a simple ML model.
Engines (E level)	Can explain how a decision tree can be used to classify items, can explain in simple terms how a neuron works with relationship to learning about ML.

Social & Ethical

The social and ethical – SE – level relates to the impact of AI systems on everyday life, and the ethical implications for wider society. Learners should consider issues such as privacy or bias, the impact of AI technologies on employment, misinformation, and the potential benefits of AI applications at this level. Leading activities or discussions focused on this level should require very little technical detail for you or your learners.

Application

The application – A – level concerns the use of AI applications and tools. Chatbot applications such as Google's Gemini or OpenAI's ChatGPT are examples of AI applications that use a large language model (LLM) to generate responses. Applications are built 'on top' of ML models using code, to make the model more accessible and useable. Teaching at this level is about the use and impact of the application, and doesn't require you to understand how specific AI systems work or how to train ML models.

Model

At the model – M – level, you cover the underlying models that are used by AI and ML applications. This includes understanding the different ways ML models can be trained, as well as the processes involved in training and testing ML models. More technical knowledge is useful to really dig into materials at this level, but an understanding of the data used (because of your subject expertise) is a great starting point.

Engine

The engine – E – level is related to the algorithms and methods (called engines) that are used to create ML models. For example, this level would include the complex technical processes used to actually create the models themselves, beyond collecting data and training them.

Using the SEAME framework

When preparing to teach a class about AI or investigate a particular AI application, you can use this framework to help you plan, by thinking about which levels to include. There are loads of interesting learning that can happen at every level. The framework allows you to design a progression for your students. For example, there is no use in jumping right to the engine level if they have no concept of what an AI application does. You can make pedagogical decisions based on the age of your learners, their prior experience with AI technologies, and your level of comfort with the particular technology you want to study.

For younger learners, exploring the social and ethical implications of tools like ChatGPT does not require an in-depth understanding of how the model works – a high-level overview of the tool will allow them to think critically about how it might impact the world around them.

You might have a particular AI application that you want to explore, such as using an image generator to make a poster about a history topic. In this case, the learners don't need to know how the developers created the image generator. They just need to explore ways to prompt and question the application to create something.

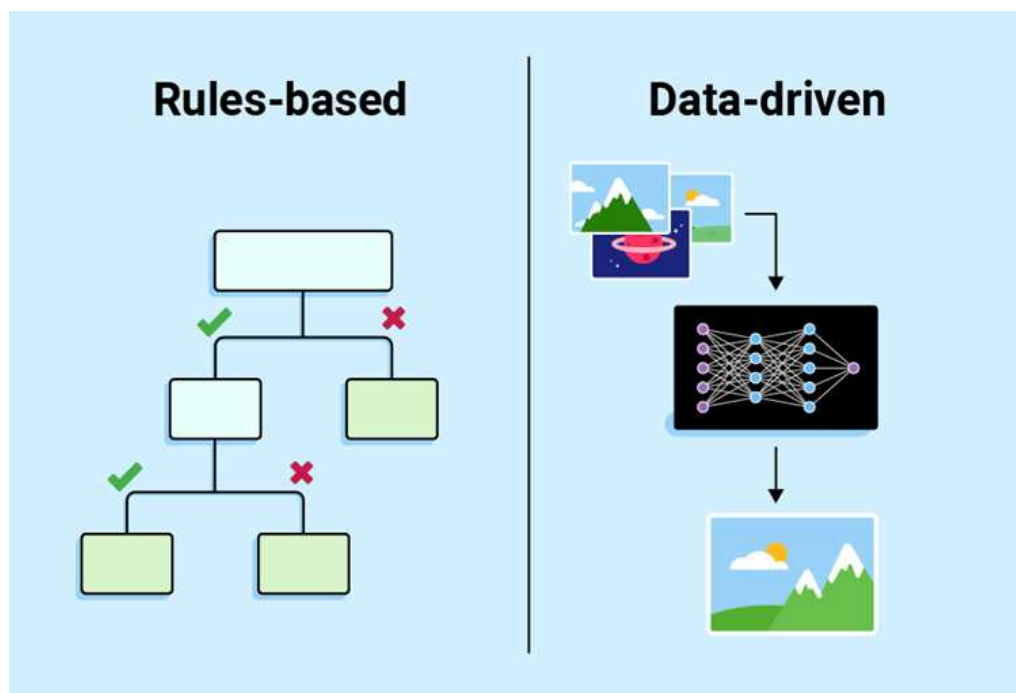
Rules-based systems

Traditional computer programming involves a coder carefully writing out lines of code – building the exact rules a piece of software uses while running. Except for the occasional bug, all the functionality and outputs have been carefully chosen and designed by the original coder (or coders).

This approach provided us with amazing technology for many years, but when tackling complex problems there are limits to this type of programming. Only functionality and outputs that the programmer can design and write out in code are possible.

As we saw earlier this week, some AI applications known as “good old-fashioned AI” or GOFAI worked on this model too. Deep Blue, the AI system that beat world champions of chess, was built on clearly programmed rules paired with loads of processing power.

Machine learning has created a new model for software engineering – a data-driven approach. This approach allows applications to produce outputs that no programmer had to pre-imagine, and has greatly expanded the problems AI can help solve.



Machine learning

To create a machine-learning application, the first thing you need is data – and lots of it. Society has become extremely skilled at collecting data so there is no shortage for programmers to build from. Once a problem has been identified, the first step is to represent that problem with data. Sometimes this data already exists, other times the data is collected from many sources.

The next step is to use machine learning to “train” a model on your data – different types of machine learning use different approaches to training.

Supervised learning involves labelling training data – we tell the model exactly what output we expect from each part of the training data. For example, an application built to recognise animals from images would use training images with the correct animal already labelled. This type is called supervised because you have to tell the model exactly what you expect from it. The model can then be used on new data and it will predict an output of one of the labels used to train it.

Unsupervised learning is another approach, which does not involve labelling the data – instead the model is trained by processing the training data and finding similarities between different items. The model will predict groups of data based on those similarities. This is a great way of

organising and understanding large data sets to find patterns, or to find ways of treating new data based on the similarities with these groups.

Reinforcement learning is a way of training a model through trial and error. The developer decides on parameters for the model to receive rewards. The model continuously receives training data as input and predicts outputs to maximise those rewards. This is how a lot of generative AI models are trained, producing media and being rewarded for high quality and convincing outputs.

This is what it means to be data driven rather than using pre-written rules; machine-learning models process data and produce outputs based on that training. This means ML models can produce outputs beyond what a human programmer might have envisioned and can account for small but important details and nuances in the data that a human programmer might not spot. This “training” based on data is the “learning” in the term “machine learning” – it’s important that you don’t confuse this learning with the type that humans do.

It’s important to note that all outputs from machine-learning models are predictions. These systems use statistics to produce the most likely output, but there is always some level of uncertainty whether it is the correct output.

Problems machine learning can’t overcome

Machine learning is far from a perfect system. There are some challenges that are particularly tricky for machine learning developers.

A machine-learning model cannot produce outputs beyond the training data – so they all have a limited scope of usefulness. If a model has been trained to recognise heart disease, then it cannot recognise other conditions. The search for more general models is ongoing, but the amount of training and processing power is limiting.

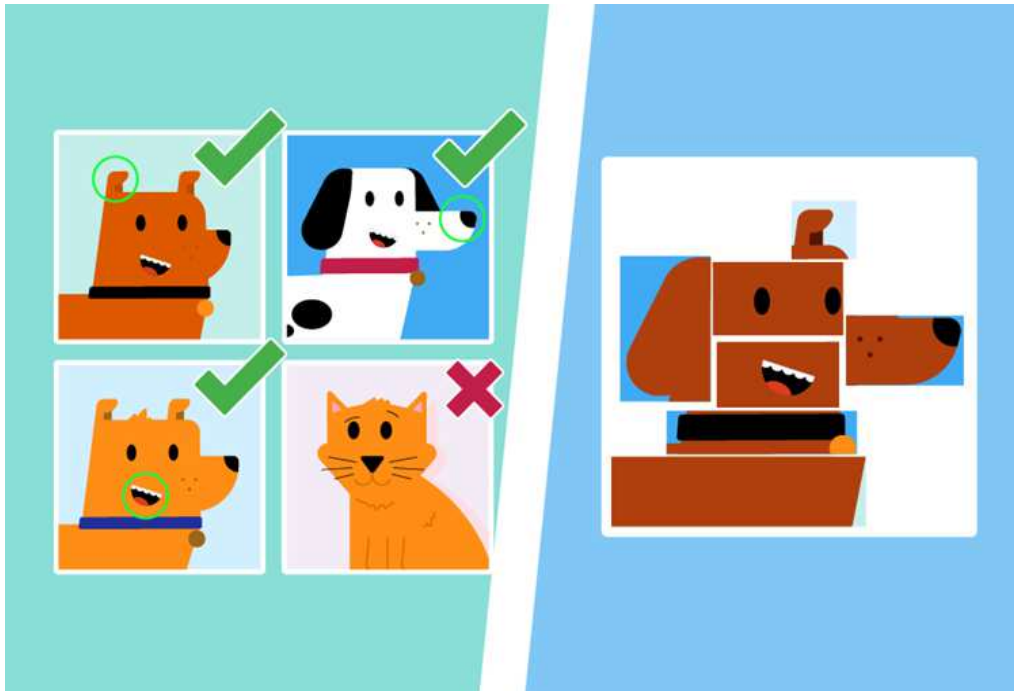
In general terms, bias refers to a prejudice in favour of or against one thing, person, or group compared with another, usually in a way considered to be unfair.

Bias in data will cause bias in the outputs of a machine-learning model. If the training data used to create a model over-represents one group of people or contains gaps, then the outputs of the model will also have the same overall bias. In creating and training models, great care has to be taken to identify and correct bias.

Predictive vs. Generative AI

Predictive AI – The pattern seeker

Predictive AI models operate by analysing existing data to identify patterns, and using those to make predictions about new data. Think of your YouTube recommendations and how they are based on your past watching habits, or self-driving cars detecting obstacles and selecting actions (braking, steering) based on previous training data.



Other examples of predictive AI in everyday life include navigation apps that analyse numerous routes to predict the fastest one based on current traffic conditions, or shopping services like Amazon and eBay that recommend products by learning shopper preferences over time. Each instance shows how predictive AI makes suggestions to help people make decisions.

Generative AI – The making machine

Generative AI extends the capabilities of artificial intelligence by processing training data to generate new, original content. Unlike predictive AI that forecasts based on known data, generative AI can create new digital artefacts such as text, images, or music that mimic the style and characteristics of the training data but are entirely new creations. This capability makes it a really exciting tool for education, where it can be used to simulate complex problem-solving scenarios or provide learners with unique, interactive learning experiences.

For instance, in the classroom, generative AI can create realistic dialogues for language learning or produce detailed visual aids that help learners visualise historical events or scientific concepts. Additionally, generative AI's ability to produce varied and complex outputs from a set of parameters means that educators can provide personalised learning materials and prompts that adapt to the needs of each student, fostering a more inclusive and effective educational experience.

Why does it matter?

Understanding the difference between predictive and generative AI is crucial for you as an educator because it directly affects how you can harness these technologies to enhance your teaching and enrich your students' learning experiences. Being empowered to discuss these

technologies confidently and authoritatively with your learners increases your credibility and enriches classroom discussions. Grasping the creative potential of generative AI allows you to bring innovative content into the classroom, sparking creativity and critical thinking among your students.

Recognising these capabilities enables you to make informed decisions about incorporating AI tools in your lessons, ensuring these technologies complement rather than complicate your teaching methods. This awareness empowers you to maintain a balanced approach to AI use in your classroom, one where technology serves as a support system that enhances interaction and engagement, rather than replaces the vital human elements of education. By effectively integrating AI, you can transform your classroom into a dynamic learning environment that prepares learners for a digital future, all while ensuring the technology is used responsibly and ethically.

Skill development for an AI-driven world

AI is becoming fundamental in many workplaces, making it crucial to develop key skills that are essential for success in an AI-driven economy. These skills help individuals not only use AI technology effectively but also think carefully about how it's applied and the implications it might have.

- **Critical thinking:** Very important for carefully evaluating what AI produces and making smart decisions based on this information.
- **Problem solving:** Learning how to break down problems and solve them step by step is crucial in using AI systems to meet various needs.
- **Creativity:** Allows for the development of new uses for AI tools in different areas and challenges.
- **Effective communication:** Working with generative AI tools requires clarity and conciseness in communication to get the right results.

Technical skills are also becoming essential in many fields. Abilities like coding and data analysis are not just for IT experts anymore. Knowing the basics of programming and how to analyse data can enable you to work effectively with AI tools and enhance their use.

- **Coding:** Gives you the tools to create and adjust AI models or to understand how these systems function.
- **Data analysis:** Important for understanding the large amounts of data that AI works with and ensuring that AI applications are accurate and trustworthy.

Ethical considerations in AI

As AI becomes a more common part of our lives and jobs, it brings with it important ethical considerations that we must address. These include issues such as data privacy, fairness in AI decisions (known as algorithmic bias), and the ethical creation and use of AI solutions.

- **Digital divide:** Imagine a situation where some people have the latest smartphones and fast internet while others don't have even a basic computer. In the world of AI, this means that people with better tech can use AI to help them with things like finding jobs, learning new skills, or getting health advice, while those without are left behind.
- **Bias:** Sometimes, AI systems can pick up unfair preferences, like favouring one group of people over another, just because of the data they were trained on. It's like if a system is trained on old books that have outdated ideas about who can do certain jobs – then, it might wrongly suggest jobs based on these old ideas.
- **Privacy:** With AI systems, there's a lot of talk about privacy because these systems need a lot of data in order to train them to make predictions. This can mean collecting details about what you do online, where you go, and even who you talk to. People worry about who can see this information and what they can do with it.
- **Job loss:** As technology gets better at doing certain jobs, there's a chance that it can replace human workers. For instance, some factories now use robots for tasks that people used to do. While AI might help create new kinds of jobs, the fear is that these jobs might not come quickly enough, or they might need skills that not everyone has.
- **AI decision making:** AI decision making is about using AI to make choices, like who gets a loan or what treatment a patient should receive. This can make things more efficient and help handle lots of data quickly, but it also means that sometimes decisions are made without a clear explanation, which can be confusing or unfair if the AI isn't checked carefully.

Guidelines for ethical use of AI applications

Ethical AI applications should be founded on four main pillars: fairness, accountability, transparency, and privacy:

- **Fairness:** AI systems should be designed to avoid unfair biases that could harm users. Developers must work to create models that treat all user groups equally. Users should make sure not to use an AI application in unintended ways – the testing process the developers use is crucial in identifying unfair results.
- **Accountability:** All stakeholders, from users to developers, must hold themselves responsible for the use of an AI system, working to maximise benefits whilst mitigating risks.
- **Transparency:** Developers should work to ensure AI systems are clearly explained and documented. A user should be able to find out where the training data came from, intended uses for a system, and how accurate that system is. As users, we should be transparent in our use of AI tools so anyone impacted can report unfair outputs to the developers.
- **Privacy:** Protecting user data is most important. AI systems must be designed to safeguard personal information and use it only in ways that users have explicitly agreed to.

Data privacy

It's not always clear exactly how training data will influence a model's output, or whether it will be replicated exactly in an output. Developers have a legal and ethical obligation to protect user data – both during training and afterwards.

Users also need to make sure they are taking steps to reduce any data privacy risks. When supplying data to AI models, we must be aware that some developers might use this data to train and improve their systems. It is crucial not to provide personal information to generative AI models. Users need to hold AI developers accountable for making their terms and conditions easy to understand; this includes providing clear ways to opt-out of data collection to protect privacy.

Using AI ethically

The young people you are educating are growing into a world that will be shaped by AI tools; this carries with it responsibilities to use these tools ethically.

Producing high-quality media has gotten easier, and so existing issues of consent are vital when using images or videos of someone else. Young people should be told to explicitly get consent before using image or video generators to make videos – even of friends.

They also need to ensure their consent is needed to access pictures of them. All too easily a young person's likeness can be taken from publicly available pictures and videos of them. Young people need to revisit their security settings to ensure only people they know can access images and videos of them.

AI applications are tools – it is how you use them that shapes the impact on people around you. Holding AI developers accountable does not mean all responsibility is taken from us. AI applications can't cause harm without people using them. Just like how we reiterate safety briefings before using chemicals in science labs – issues of ethics should always accompany lessons on AI tools.

Addressing education-related fears and challenges

Overcoming the fear of AI-enhanced cheating

Challenge: There's a common concern that learners might use AI tools to sidestep traditional learning paths, turning to technology to complete assignments unethically.

Opportunity: This challenge presents a unique chance to reinvent how we assess student understanding and creativity. Instead of traditional tests and essays, think about assigning projects that require a personal touch, like video essays, podcasts, and live presentations. These formats not only make cheating difficult, but also encourage learners to use AI as a tool for researching and enhancing their own original ideas rather than replacing them.

Example: Consider a history class where learners are tasked with creating a documentary about a historical event using AI tools to gather information and create initial scripts, but then must personalise their narrative, critique their sources, and present their unique viewpoint. This method evaluates critical thinking, creativity, and the ability to engage with technology ethically and effectively.

Addressing concerns about AI replacing educators

Challenge: Concern is being raised in the media that AI might make educator's roles redundant, fearing a future where technology overtakes the human touch that is essential in teaching.

Opportunity: Rather than viewing AI as a competitor, it should be seen as a complement to the teaching process. AI applications can help with time-consuming tasks like creating quizzes and generating diverse instructional materials, allowing educators more freedom to focus on what really matters – interacting with students, providing personalised feedback, and developing innovative teaching strategies.

Example: Teachers at King Egbert School exemplify how AI tools can tailor educational materials, such as creating precise visuals for language lessons. More broadly, a UK Department for Education report reveals that many educators are using AI to reduce administrative tasks like grading, freeing up more time for interactive teaching.

Encouraging responsible AI use among students

Challenge: There's a risk that learners might become overly reliant on AI, using it as a crutch rather than a tool, which could potentially undermine their learning process.

Opportunity: This is an excellent moment to teach digital literacy and ethics. Educators can design activities where AI tools are used as a starting point for assignments that still require significant student input and critical thinking to complete. This encourages learners to interact with AI critically, recognising its limitations and learning to value their own insights and contributions.

Example: You could implement a class session where learners use AI to generate a draft for a research project, but then must evaluate the AI application's work, identify any biases or errors, and refine the final product with their analysis. This not only teaches them about the technology's capabilities and limitations but also enhances their analytical skills.

Transforming challenges into opportunities

As we navigate these challenges, the focus should not be on what AI can replace, but on how it can enrich and expand the educational experience. By shifting our perspective from fear to opportunity, we can ensure that AI serves as a bridge to more innovative, engaging, and personalised learning environments.

Sources: HP AI Teacher Academy, Teach Teens Computing: Understanding AI for Educators course by the Raspberry Pi Foundation (open source)

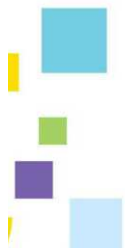
ANNEX 4

Glossary of Terms

1. AI – artificial intelligence – the field of technology focused on creating computer systems that can perform tasks that normally require human intelligence, such as understanding language, recognising patterns, solving problems, or making decisions.
2. AI generated image – a picture created or modified by artificial intelligence, typically using machine-learning models that produce visuals from text descriptions or other input data.
3. Bias – an unfair or unbalanced preference or prejudice that affects judgment, decisions, or outcomes, often without conscious awareness.
4. Clickbait – online content – usually headlines or thumbnails – designed to attract attention and entice users to click, often by using sensational, misleading, or exaggerated claims.
5. Clickjacking – Tricking users into clicking on malicious content.
6. Cybersecurity – Protecting computers, networks, and data from digital threats.
7. Data Privacy – Protecting personal and student information.
8. Data Protection – Keeping information safe according to privacy laws.
9. Deepfake – synthetic media – usually videos, images, or audio – created or altered using AI to convincingly mimic a real person’s appearance or voice.
10. Digital Footprint – The trail of information you leave online.
11. Doxing – the act of publicly revealing someone’s private or identifying information online without their consent, often with harmful intent.
12. Educator – anyone who supports learning and development – not only teachers, but also parents, coaches, scout leaders, mentors, and other adults who guide, teach, or influence young people.
13. Encryption – Turning data into a code to prevent unauthorised access.
14. Fake news – false or misleading information presented as legitimate news, often created to influence opinions, deceive audiences, or generate clicks.
15. Firewall – A system that blocks unauthorised access.
16. Gaslighting – a form of psychological manipulation where someone causes another person to doubt their own memory, perception, or sanity in order to gain control or avoid accountability.

17. GDPR – General Data Protection Regulation – a European Union law that sets rules for how organisations collect, use, store, and protect people’s personal data, giving individuals strong rights over their own information.
18. Generative AI – a type of artificial intelligence that can create new content – such as text, images, audio, or code – based on patterns it has learned from data.
19. Grooming – the process in which someone builds trust with a minor or vulnerable person, often online, with the intent to exploit or harm them, typically for sexual or other abusive purposes.
20. Incident Response – Steps taken to manage and recover from a cyberattack.
21. LLM (Large Language Model) – a type of AI system trained on massive amounts of text data to understand and generate human-like language, allowing it to answer questions, write content, and engage in conversation.
22. Malware – Malicious software like viruses or ransomware.
23. Manipulation – the act of influencing or controlling someone’s thoughts, emotions, or actions in a deceptive or unfair way, often for personal gain.
24. Manipulation – the act of influencing or controlling someone or something in a deceptive, unfair, or hidden way – usually to serve one’s own interests at the expense of others.
25. Misinformation – Misinformation is false or inaccurate information.. For example, a relative might share a health “tip” on social media, believing it to be helpful, even though it is not based on evidence.
26. Disinformation – false information which is deliberately intended to mislead – intentionally misstating the facts. It is deliberate misinformation. This includes conspiracy theories, manipulated videos, or propaganda campaigns.
27. Parent – any primary caregiver responsible for a child’s wellbeing and development, including biological, adoptive, and foster parents, as well as guardians, stepparents, and other adults who take on a parental role in a child’s life.
28. Password Hygiene – Best practices for creating and managing strong passwords.
29. Patch/Software Update – Updating software to fix security problems.
30. Phishing – Tricking people into giving up private information via fake communications.
31. Post-truth – a situation where emotional appeal and personal belief have more influence on public opinion than objective facts, making truth less central in shaping views and decisions.
32. Predictive AI – artificial intelligence designed to analyse data and forecast future outcomes or behaviours, such as trends, risks, or user actions.
33. Ransomware – Malware that locks your files and demands payment.

- 34. Safe Browsing – Avoiding dangerous websites and downloads.
- 35. School leader – anyone who holds a leadership role in a school – such as heads, principals, directors, deputy leaders, department heads, or coordinators – responsible for guiding the school's vision, policies, and overall environment.
- 36. Social Engineering – Manipulating people into giving up confidential information.
- 37. Spam – Unwanted digital messages, often containing scams or malware.
- 38. Spyware – Software that secretly collects your information.
- 39. Two-Factor Authentication (2FA) – Requiring two types of verification to log in.
- 40. VPN (Virtual Private Network) – A secure internet connection that protects your data.
- 41. Whole school approach – a strategy where everyone in a school – students, teachers, staff, leadership, families, and the wider community – works together to promote a shared goal, such as wellbeing, safety, or learning improvement. It integrates policies, practices, and culture across the entire school.
- 42. Zero-Day Attack – A cyberattack that exploits a brand-new vulnerability.




101132954 | DRONE |
ERASMUS-EDU-2023-PI-FORWARD



The DRONE Consortium

 HELLENIC OPEN UNIVERSITY	HOU	HELLENIC OPEN UNIVERSITY	https://www.eap.gr/en/shu/
 CMT Prooptiki CONSULTING MANAGEMENT TRAINING	CMT	C.M.T. PROOPTIKI CONSULTING MANAGEMENT TRAINING EPE	https://cmtprooptiki.gr
 ELTE EOTVOS LORAND UNIVERSITY	ELTE	EOTVOS LORAND TUDOMANYEGYETEM	https://www.elte.hu/en/
 esha European School Heads Association	ESHA	EUROPEAN SCHOOL HEADS ASSOCIATION	http://www.esha.org/
 CPI CYPRUS PEDAGOGICAL INSTITUTE	CPI	PAIDAGOGIKO INSTITOUTO KYPROU	https://www.pi.ac.cy/pi/
 PARENTS INTERNATIONAL	IPA	STICHTING INTERNATIONAL PARENTS ALLIANCE	https://parentsinternational.org/
 UNIVERSITY of NICOSIA	UNIC	EDEX - EDUCATIONAL EXCELLENCE CORPORATION LIMITED	https://www.unic.ac.cy/
 Politecnico di Torino	POLITO	POLITECNICO DI TORINO	https://www.polito.it/

Associated Partner

 ЛЕСЬКА УКРАЇНКА ВОЛЫН НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ LESYA UKRAINKA VOLYN NATIONAL UNIVERSITY	LUVNU	LESYA UKRAINKA VOLYN NATIONAL UNIVERSITY	https://vnu.edu.ua/en
--	-------	---	---

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.



**Co-funded by
the European Union**