DIGITAL PATHFINDER

DRONE Handbook for School Leaders

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.

Editor: Judit Horgas

Design: Emanuele Bertolani

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

This handbook is designed as a strategic and operational guide to shaping your school's digital culture. It supports school leaders in shaping whole-school digital culture, safeguarding practices, staff development, and responses to disinformation and digital risk.

Digital literacy in schools is no longer optional but rather a core element of school leadership – it affects wellbeing, trust, teaching quality, and the school's public reputation. This handbook helps senior leaders address these challenges proactively and responsibly.

How to get the most out of it

Start with the strategic overview: use the introduction and first chapters to understand the broader implications of digital literacy for school culture, policy, and leadership responsibility.

1. Assess your leadership strengths and gaps. Reflection tools help identify areas for improvement:

- Risk assessment processes
- Staff training needs
- Cybersecurity preparedness
- Communication systems
- Digital tool and platform evaluation

Use this to identify priorities and allocate responsibilities.

2. Use chapters as action frameworks. Each chapter includes practical steps, policy considerations, and scenarios you can use to inform leadership decisions, risk assessments, and school-wide planning.

3. Support staff development. Use the teacher-focused strategies to design CPD sessions, mentoring programmes, and collaborative learning initiatives.

4. Strengthen whole-school systems. The handbook includes guidance for:

- developing or updating anti-bullying policies
- evaluating digital tools and external partnerships
- setting clear expectations for staff conduct
- building resilient communication systems with families
- preventing and responding to misinformation crises

5. Learn from the case studies. Case studies are based on real situations faced by schools. They can be used for leadership team discussions, staff training, and scenario planning.

6. Revisit during crises. When an incident occurs, misinformation, cyberbullying, platform misuse, the "when things go wrong" sections provide immediate steps for stabilising the situation.

A leadership resource

This handbook supports you in creating a safe, ethical, future-ready digital environment. Use it to strengthen staff confidence, protect students, build trust with families, and make informed decisions in a rapidly changing digital landscape.

If You Want to Go Deeper

Leadership modules in the DRONE online course provide advanced guidance on crisis communication, digital safeguarding, and strategic planning.

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)

WHAT DO I NEED RIGHT NOW?

PATH 1
Build leadership in digital literacy

- **INTRODUCTION** The role of school leaders (p.13)
- **CHAPTER 1** Information literacy (pp.17-26)
- **CHAPTER 2** Disinformation, misinformation & fake news (pp.27-34)

PATH 2
Build resilience and problem-solving skills

- **CHAPTER 3** Resilience Building (pp.35-44)
- **CHAPTER 4** Problem-solving (pp.45-54)

PATH 3
Deal with concrete risks & incidents

- **CHAPTER 6** Bullying and Cyberbullying (pp.67-78)
- **CHAPTER 7** Cybersecurity (pp.79-88)
- **TOOLBOX GUIDES** (pp.107-124)

PATH 4
Build Policies and Alliances

- **CHAPTER 5** Critical thinking (pp.55-64)
- **CHAPTER 8** Building Alliances (pp.89-98)
- **TOOLBOX GUIDES** (pp.107-124)

Introduction: Digital Literacy and Disinformation: The Role of Schools

In today's world, digital environments shape almost every aspect of young people's lives. Students learn, communicate, play, and even build their sense of self in spaces that are mediated by technology. This digital reality brings enormous opportunities: access to knowledge, creative expression, and global collaboration. Yet it also carries serious risks. Among the most pressing of these is the spread of misinformation, disinformation, and harmful content.

Schools sit at the heart of this challenge. They are not only centres of academic learning but also critical spaces where students can develop the habits, skills, and resilience needed to navigate a digital society. Unlike informal online environments, schools provide structured opportunities for questioning, reflection, and critical engagement with information. They can function as protective environments where misinformation is challenged, fake news is unpacked, and young people learn to participate responsibly in digital communities.

Within this context, school leaders play a pivotal role. They set the direction of the school, define priorities, and establish the culture within which teachers and students interact. When school leaders treat digital literacy as essential, it becomes embedded across the curriculum, the pastoral system, and the wider life of the school. Conversely, if leadership overlooks these issues, gaps open up that can leave students unprepared, teachers unsupported, and communities vulnerable.

Why Digital Literacy Matters for School Leaders

Digital literacy is often misunderstood as a purely technical matter: knowing how to operate devices, log into platforms, or use specific applications. In reality, it is far broader. Digital literacy encompasses the ability to search, evaluate, interpret, and respond to information. It requires both critical and ethical awareness – knowing not only how to use technology but also why, when, and with what consequences.

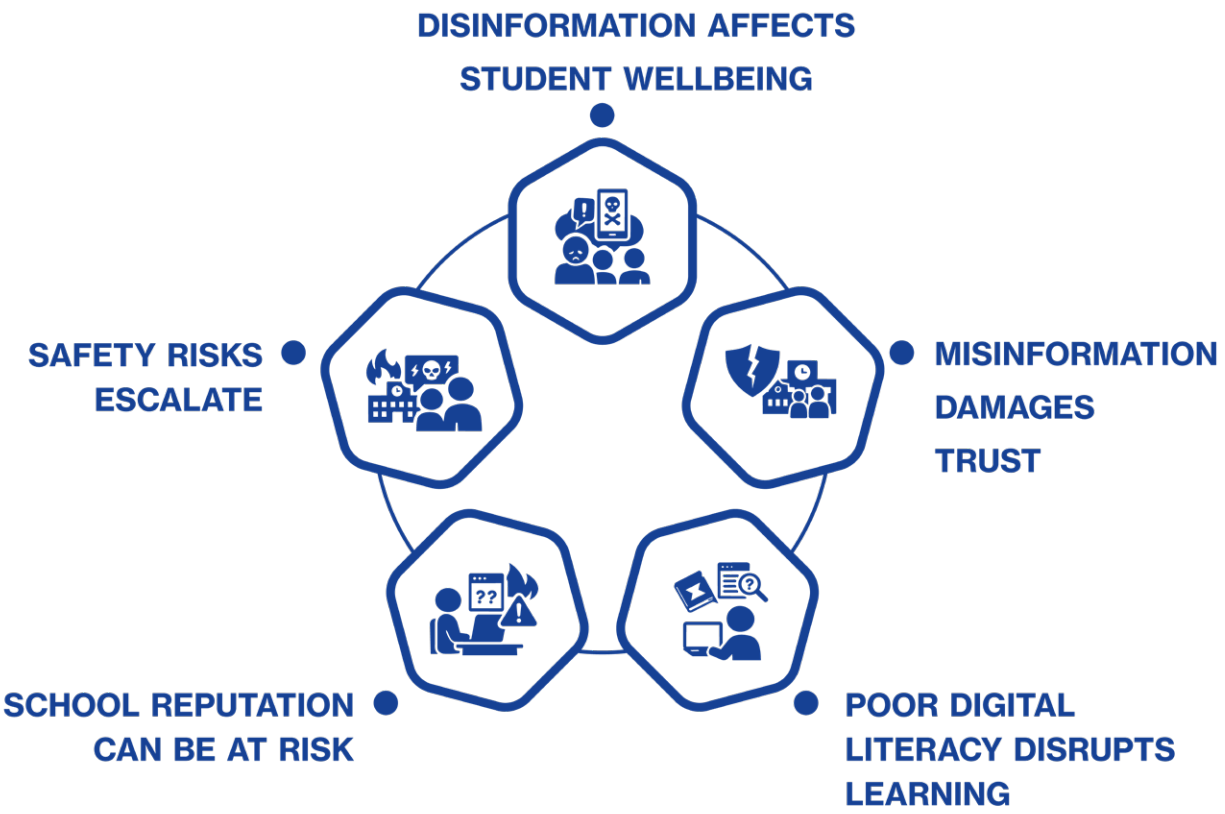
For school leaders, this matters in several ways:

- Disinformation affects student wellbeing. A false story circulating on social media can cause anxiety, exclusion, or division among students. Young people who cannot distinguish reliable from unreliable content are more likely to feel insecure or manipulated.
- Misinformation can damage trust between schools and parents. When rumours spread unchecked – for example, about curriculum changes, health policies, or disciplinary practices – they undermine confidence in the school community.

- Poor digital literacy can disrupt learning. Students who lack the ability to filter information may rely on unreliable sources in their assignments or bring harmful narratives into classroom discussions.
- School reputation is at risk. A single piece of false information about a school can spread quickly online, creating public relations crises that distract from learning and consume staff energy.
- Safety risks escalate. Disinformation is not only about misleading news; it also includes harmful challenges, hoaxes, or scams targeted at young people. Without digital literacy, students are more vulnerable to these risks.

In short, digital literacy is not an optional extra for schools. It is a fundamental competence that underpins academic achievement, community cohesion, and student safety. School leaders, by acknowledging this, can steer their schools towards a future where digital environments are navigated critically, responsibly, and safely.

WHY DIGITAL LITERACY MATTERS FOR SCHOOL LEADERS



The Role of School Leaders in Fostering Digital Literacy

Because digital challenges touch every aspect of school life, fostering digital literacy requires more than a few lessons on online safety. It requires systemic leadership. School leaders must:

1. **Establish clear policies and procedures.**
   A whole-school approach means embedding digital literacy into safeguarding policies, curriculum frameworks, and codes of conduct. This ensures consistent expectations across classrooms, year groups, and extracurricular activities.

2. **Support and resource teachers.**
   Teachers are on the frontline of digital literacy education, yet many feel underprepared. School leaders must ensure access to training, provide time for professional development, and integrate digital literacy into broader teaching priorities.

3. **Model responsible digital engagement.**
   Leaders' own communication – whether through newsletters, social media, or responses to crises – sets the tone. Transparent, evidence-based, and respectful engagement shows students, staff, and parents what critical digital practice looks like in action.

4. **Build partnerships with parents and the community.**
   Digital literacy cannot be taught in isolation at school. Parents and carers play a crucial role in shaping children's digital habits. School leaders should actively engage families, offering workshops, resources, and open communication to align efforts across home and school.

5. **Collaborate with technology providers carefully.**
   Schools increasingly rely on digital platforms and services, from learning management systems to educational apps. Leaders must evaluate these relationships critically, ensuring that contracts respect student privacy and that platforms serve educational rather than purely commercial interests.

Through these roles, school leaders transform digital literacy from an abstract ideal into a lived reality for students and teachers.

Whenever you review your school's digital literacy vision, crosscheck it with your national or regional digital education and child protection strategies. This ensures that local initiatives strengthen, rather than duplicate or contradict, existing policy frameworks.

When defining digital priorities, school leaders should explicitly check whether proposed tools and practices are consistent with the school's value compass, as highlighted in **ESHA's HEADstart #4**. This means weighing not only technical benefits, but also the fairness, inclusion, and long-term ethical impact of each digital decision.

Competence Development and Support Needs: Insights from DRONE Research

The DRONE project highlights a recurring challenge: while school leaders recognise the importance of digital literacy, many feel underprepared for the complexity of the issues. This gap is not due to lack of commitment but to the sheer pace of change. New platforms, apps, and risks emerge faster than policies and training can adapt.

DRONE findings point to several areas where school leaders particularly need support:

- Frameworks for embedding digital literacy into curriculum design. Many leaders want to go beyond piecemeal lessons and integrate digital literacy across subjects, but they lack clear models for doing so.
- Guidance for responding to disinformation in the school community. Leaders often encounter rumours, false claims, or manipulated content but are unsure how to respond in ways that calm rather than inflame tensions.
- Practical tools for supporting teachers. Leaders need ready-to-use resources, professional development modules, and case studies that can be adapted to their school context.
- Confidence in their own digital skills. Leaders themselves sometimes struggle with evaluating online information, managing social media communications, or understanding cybersecurity basics. Professional development for leaders is therefore just as important as for teachers.

The DRONE research suggests that effective leadership in this area requires humility as well as authority: recognising gaps in one's own competence, being willing to learn alongside staff, and creating a culture where digital literacy is a shared journey.

Case Study: "Rumours in the Community"

A medium-sized secondary school faced a crisis when a rumour spread rapidly on local social media groups. Parents were claiming that the school intended to cancel a popular extracurricular programme due to budget cuts. The rumour, shared by a single account, quickly gained traction and caused anger. Staff began receiving frustrated emails from parents, and students worried they were about to lose an important activity.

The school principal acted quickly. First, she verified the facts internally and confirmed that no cancellation was planned. Next, she issued an official statement through the school's website, newsletter, and social media channels. The message not only clarified the misinformation but also explained how the rumour had arisen from a misinterpreted budget line in a public report. Finally, she invited parents to an open meeting to discuss school funding priorities transparently.

This approach achieved three things:

- It calmed the immediate crisis, preventing further conflict.
- It restored parent trust, showing that the school responded openly and respectfully.
- It modelled critical digital engagement, demonstrating to students how to respond to false information with evidence, clarity, and dialogue.

The case illustrates how school leaders, by acting decisively and transparently, can turn a potential crisis into an opportunity for teaching and trust-building.

Conclusion

Digital literacy and disinformation are not peripheral concerns for schools; they are central to education in the 21st century. For school leaders, the responsibility is twofold: to protect students and staff from the harms of misinformation and to empower them with the skills and confidence to navigate digital environments responsibly.

This requires leadership that is proactive, systemic, and collaborative. It requires school leaders to:

- Recognise the far-reaching impacts of digital literacy on learning, wellbeing, and trust.
- Embed digital safety and competence into school policies, culture, and daily practice.
- Support teachers with training, resources, and encouragement.
- Engage parents and communities as partners in digital education.
- Continuously develop their own digital competences, modelling the values they seek to instil.

The DRONE project underscores that leaders cannot solve these challenges alone, nor do they need to. By building alliances, fostering openness, and embracing their role as digital mentors, school leaders can transform schools into communities that not only resist disinformation but also nurture informed, resilient, and critically engaged citizens.

CHAPTER 1

INFORMATION LITERACY

What Is Information Literacy?

Information literacy is the ability to find, evaluate, interpret, and use information effectively. In practice, it means asking questions like:

- Who created this information, and why?
- What evidence supports it?
- How current is it?
- What perspectives or biases are present?
- How can this information be applied responsibly in a school context?

In a world of instant messages, viral posts, and algorithm-driven feeds, information literacy is no longer an optional academic skill; it is a survival skill. For schools, it underpins not only classroom learning but also student wellbeing, staff professionalism, and community trust.

School leaders must understand that their role is not simply to ensure students have access to information. Rather, their task is to cultivate a school-wide culture of critical engagement, where both staff and students can question, verify, and apply information in thoughtful and ethical ways.

Developing Your Information Literacy Competences as a School Leader

Before supporting others, leaders need to examine their own competences. Research from the DRONE project shows that many school leaders feel less confident in evaluating online content than in managing traditional school policies. The first step is self-assessment.

A Self-Reflection Test

School leaders can ask themselves:

1. When I read a news story online, do I automatically check the source?
2. Can I identify the difference between a fact-based report and an opinion piece?
3. Am I aware of the signs of manipulated images or "deepfake" videos?
4. Do I feel confident responding to parents or students who share false claims?
5. When I make decisions, do I rely on a range of trusted sources rather than a single channel?

If the honest answer to several of these questions is "no" or "not sure," then professional development in information literacy is not just advisable – it is urgent.

Practical Steps for Leaders

- Engage in training: Participate in online courses or workshops that develop digital and information literacy skills.
- Model fact-checking: Share examples with staff of how you verified a story or corrected an error.
- Use multiple sources: When presenting data to staff or parents, cite more than one reputable source.
- Stay current: Follow educational organisations, fact-checking sites, and research centres that monitor misinformation trends.

Map your own professional learning against national teacher and schoolleader competence frameworks for digital or media literacy. Using these reference points helps you prioritise development areas that inspection bodies and ministries already highlight as strategic.

Supporting Teachers in Promoting Information Literacy

Teachers are the frontline educators for digital skills. However, many lack structured approaches or confidence in embedding information literacy into everyday teaching. Leaders can take several actions to ensure consistent and effective practice across the school.

Creating a School-Wide Approach

- Curriculum Integration: Embed information literacy into multiple subjects, not just ICT. For example, history teachers can compare sources, while science teachers can analyse claims about health or climate.
- Professional Development: Offer training sessions and resources on evaluating online content, teaching source analysis, and recognising manipulated media.
- Resource Hubs: Create a shared digital hub where teachers can access fact-checking tools, checklists, and lesson plans.
- Encouragement of Peer Learning: Promote teacher collaboration, where staff share classroom strategies that worked well.

Example: Whole-School Literacy Day

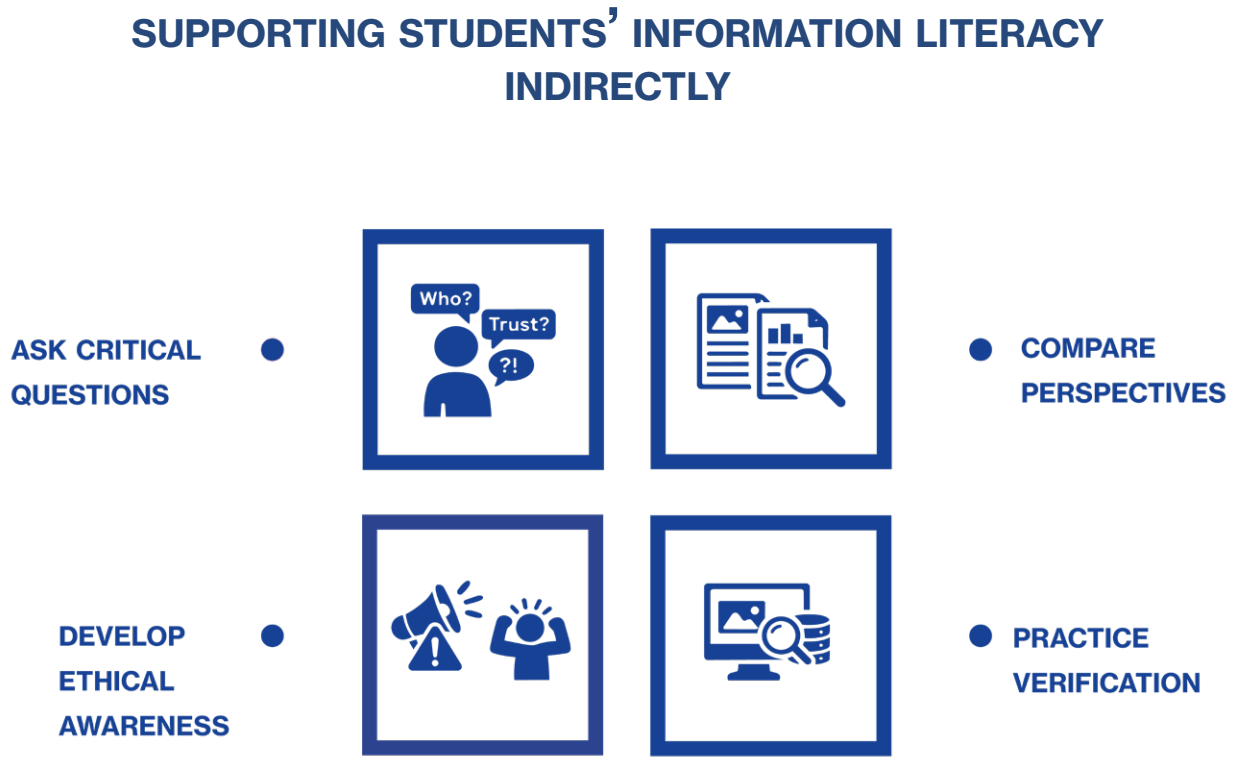
A primary school headteacher organised a “Digital Literacy Day” where every subject incorporated a critical information exercise. Maths lessons included spotting errors in graphs, English lessons compared media headlines, and art lessons examined image manipulation. Teachers reported increased student engagement and a clearer understanding that questioning information applies across disciplines, not just in IT classes.

Supporting Students' Information Literacy Indirectly

Although school leaders usually do not teach daily lessons, they have an important role in setting the conditions under which students learn. By ensuring that curricula, resources, and teacher training are aligned, leaders make it possible for students to:

- Ask critical questions: "Who said this?" "Can I trust it?"
- Compare multiple perspectives: recognising that different sources may frame events differently.
- Practise verification: learning how to use fact-checking websites, reverse image search, and reliable databases.
- Develop ethical awareness: understanding the impact of sharing false or harmful content.

Leaders who create space for these practices ensure that information literacy becomes a core competence for students, not an optional add-on.



When Things Go Wrong – From Challenges to Crises

Despite best efforts, schools will face incidents where poor information literacy causes disruption or harm.

Common Scenarios

- Rumours among students: A viral video or post sparks anxiety or conflict in school.
- Misinformed parents: Families share and act on false information about school policies.
- Staff challenges: A teacher unknowingly uses unreliable sources in class or shares unverified content online.
- Reputation crises: A misleading story about the school spreads locally or nationally.

Steps for Leaders to Respond

1. Verify Quickly: Gather facts before responding publicly.
2. Communicate Clearly: Share verified information with students, staff, and parents through official channels.
3. Educate: Use incidents as learning opportunities – explain how misinformation spread and what can be learned from it.
4. Support Staff and Students: Provide emotional support if misinformation caused distress.
5. Review Policies: After a crisis, assess whether clearer guidelines or training could have prevented escalation.

Case Study: "The Fake Health Notice"

At a secondary school, a fabricated health notice circulated on WhatsApp, claiming that the school had detected a serious outbreak and was closing. Panic spread quickly among students and parents, and local news outlets began making inquiries.
The headteacher acted swiftly:

- Confirmed facts with local health authorities.
- Issued a statement on all official channels clarifying that the message was false.
- Contacted parents via text and email to reassure them directly.
- Held an assembly where students discussed how the rumour spread and how it could have been verified.

By treating the incident not only as a crisis but also as a teachable moment, the school turned disruption into an opportunity for growth. Parents later expressed appreciation for the transparent and proactive communication.

Practical Tools for School Leaders

Information Literacy Checklist for Leaders

- I verify information before sharing it with staff, parents, or students.
- I can identify at least three trusted sources for educational and school policy updates.
- I model critical engagement with information in my communications.
- Teachers in my school have access to resources and training on information literacy.
- Our curriculum integrates information literacy across subjects.
- We have a clear plan for responding to misinformation crises.

Recommended Tools and Resources

- Fact-checking websites: Snopes (https://www.snopes.com/), Full Fact (https://fullfact.org/), EU vs Disinfo, (https://euvsdisinfo.eu/).
- Reverse image search: Google Images (https://images.google.com/), TinEye (https://tineye.com/).
- News literacy resources: News Literacy Project, UNESCO digital literacy framework.[1]
- SAILS project tools: Practical classroom checklists and information literacy self-assessments. (https://library.parenthelp.eu/captains-handbook-sails-resource-for-school-leaders/, https://library.parenthelp.eu/seafarers-guide/).

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

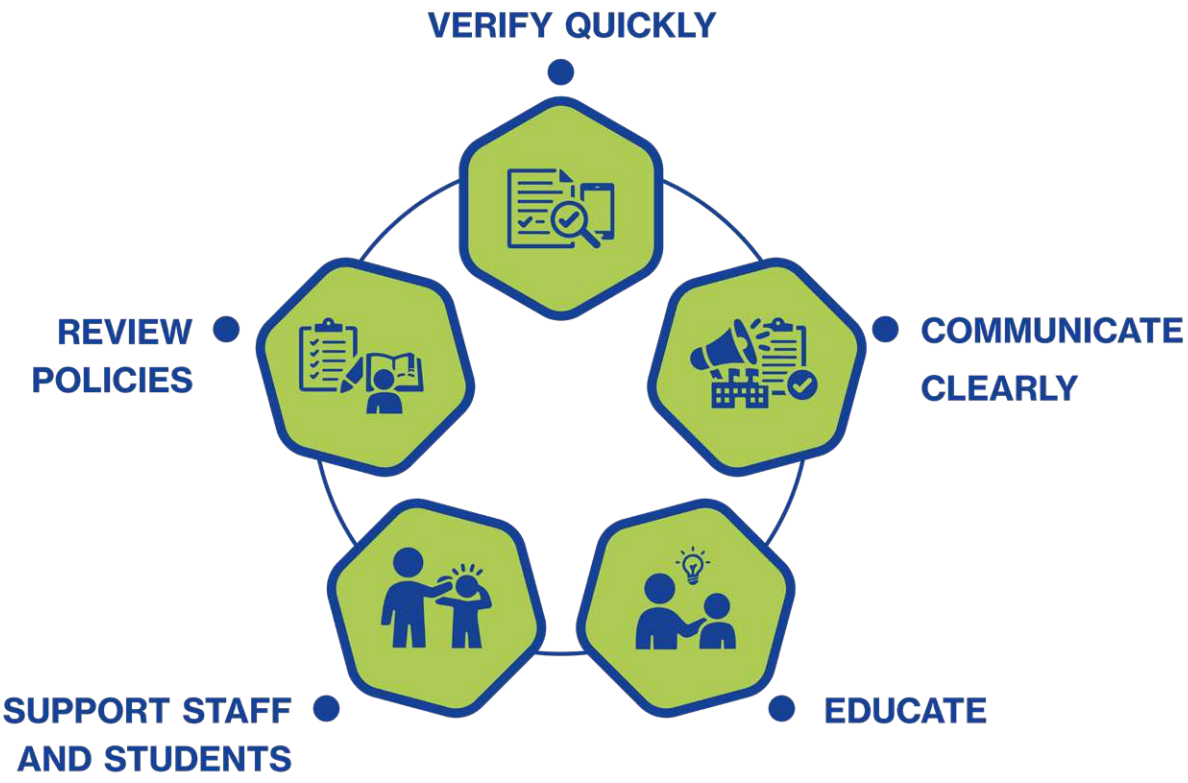
Conclusion

Information literacy is not just another skill for students to master. It is the foundation of safe, critical, and informed participation in digital life. For school leaders, building information literacy means:

- Developing their own competences.
- Equipping teachers with training and tools.
- Embedding critical engagement across the curriculum.
- Responding swiftly and effectively when misinformation causes disruption.

When leaders champion information literacy, they not only safeguard their school communities against the risks of misinformation but also nurture a culture where truth, inquiry, and trust are valued. This is not simply a defensive act – it is an act of leadership that prepares young people to thrive in an uncertain and information-rich world.

HOW TO RESPOND TO POOR INFORMATION LITERACY



CHAPTER 2

DISINFORMATION, MISINFORMATION AND FAKE NEWS

Understanding Disinformation, Misinformation, and Fake News

Although often used interchangeably, the terms disinformation, misinformation, and fake news describe distinct – and important – phenomena:

- **Misinformation**: Misinformation is false or inaccurate information. Example: a parent forwarding a viral post about a "new homework policy" they believe is real but isn't.
- **Disinformation**: false information which is deliberately intended to mislead – intentionally misstating the facts. It is deliberate misinformation. Example: a coordinated campaign that spreads false stories about a school's performance to discredit leadership.
- **Fake News**: a colloquial term used broadly to describe fabricated stories presented as real news. It can include both misinformation and disinformation.

In the context of schools, these issues are not abstract. They affect student wellbeing, community trust, staff morale, and institutional reputation. School leaders need a nuanced understanding of how these forms of false information circulate – and how to respond.

Why This Matters for School Leaders

Disinformation and misinformation impact schools at multiple levels:

1. For Students:
   - Exposure to misleading or harmful online content can distort their worldview.
   - Viral hoaxes can cause fear (e.g., "dangerous challenges") or encourage risky behaviour.
   - False claims about peers or teachers can fuel bullying or social exclusion.
2. For Parents and the Community:
   - Misinformation about school policies (e.g., curriculum, health rules, or funding) can trigger unnecessary anger or anxiety.
   - False stories can erode trust between families and the school.
3. For Staff and Leadership:
   - Teachers may inadvertently share false information with students.
   - Leaders may be targeted directly by disinformation campaigns that question their competence or decisions.
   - Reputational damage can spread quickly online, creating crises.

For these reasons, addressing disinformation is not only about protecting students – it is a leadership responsibility that extends to communication, governance, and culture-building.

Developing Leaders' Skills in Recognising False Information

Leaders cannot model resilience or support teachers if they lack confidence in recognising disinformation themselves. A strong foundation begins with building personal skills.

Key Questions to Ask When Evaluating Information

1. Source: Who published this? Is the source credible?
2. Purpose: Was this created to inform, persuade, entertain, or deceive?
3. Evidence: Does the content cite reliable data, or rely on emotion and anecdote?
4. Timeliness: Is it recent? Old news stories are often recycled as "current."
5. Verification: Can this information be cross-checked with another reputable source?
6. Language and Tone: Does it use dramatic, sensationalist, or divisive language to provoke emotion?

Practical Actions for Leaders

- Test yourself regularly: Use online games and training tools (e.g., "Bad News" by DROG, which simulates disinformation tactics - https://www.getbadnews.com/en/play- available in many languages).
- Follow fact-checkers: Subscribe to newsletters from reputable organisations such as Full Fact (https://fullfact.org/), Snopes (https://www.snopes.com/), or EU vs Disinfo (https://euvsdisinfo.eu/).
- Stay updated: Track national or local education authorities for verified guidance to avoid reliance on unverified rumours.

By improving their own critical engagement, leaders can act confidently when confronted with questionable information.

When designing schoollevel guidance on disinformation, align your procedures with any national medialiteracy or strategic communication guidelines issued for schools. Referencing these documents makes it easier for staff and parents to see that your approach follows recognised standards.

Helping Teachers Identify and Address False Information

Teachers are often the first to encounter disinformation in the classroom. Students may repeat rumours they see on TikTok, cite dubious websites in assignments, or share manipulated images in group chats. School leaders must equip teachers with strategies and confidence to respond.

Strategies for Leaders to Support Teachers

1. Training Workshops: Offer regular sessions on how to identify misinformation, including practical exercises with real-world examples.

2. Provide Resources: Develop or share checklists, fact-checking tools, and guidelines for use in lessons.

3. Create Safe Spaces: Encourage teachers to discuss challenges openly. Staff should feel safe admitting, "I'm not sure if this is true — let's check together."

4. Encourage Integration Across Subjects: Information literacy should not be isolated in ICT. Science, history, and even art lessons provide opportunities to critically evaluate sources and images.

Example: Classroom Resource Pack

One school leader collaborated with teachers to create a "Source Detective Toolkit," which included:

- A flowchart of questions for evaluating sources.
- Links to child-friendly fact-checking websites.
- Example assignments that reward critical questioning, not just correct answers.

Teachers reported higher confidence, and students became more reflective about the sources they used in projects.

Responding When Things Go Wrong

Despite proactive measures, disinformation incidents will occur. What matters is how schools respond.

Steps for Leaders in Crisis Situations

1. Verify Quickly: Establish the facts before responding publicly.
2. Communicate Transparently: Share verified information through official school channels (website, newsletter, parent app).
3. Engage Directly: If parents are concerned, organise a meeting or Q&A session to address rumours openly.
4. Support Staff: If a teacher has been undermined by disinformation, back them up publicly and privately.
5. Educate the Community: Use the incident as a teaching opportunity for students and staff about how disinformation spreads.

Long-Term Preventive Measures

- Establish a “rumour response protocol” so that staff know how to escalate issues quickly.
- Train staff in crisis communication to ensure consistency and calm messaging.
- Build partnerships with local media and parent groups, so that trusted channels exist for clarifying issues.

Case Study: "The Curriculum Controversy"

A secondary school introduced a new citizenship module focusing on media literacy. Almost immediately, false claims began spreading in the community: some parents were told (via a viral Facebook post) that the school was "indoctrinating" students with political views.
Within days, emails and angry calls began flooding the school office. Some parents threatened to withdraw their children.

Leadership Response

- The headteacher issued a clear, evidence-based statement explaining the curriculum changes, including links to official education policy.
- A parent information evening was organised, where teachers presented lesson content transparently and addressed concerns directly.
- In assemblies, students discussed how the rumour had spread and why checking sources matters.

Outcome

The proactive response calmed tensions. Parents appreciated the transparency, staff felt supported, and students learned first-hand how misinformation can distort reality. The incident became a teaching opportunity rather than a crisis.

Practical Tools for School Leaders

Misinformation Red Flag Checklist

- The story has no clear author or source. ☐
- The language is emotional, sensationalist, or divisive. ☐
- The content cannot be verified by at least one other credible source. ☐
- The images or videos may appear altered or lack context. ☐
- The story is being shared primarily on private groups or anonymous accounts. ☐

Action Checklist for Leaders

- I have trained staff in recognising misinformation and disinformation. ☐
- Our school has a clear communication plan for responding to rumours. ☐
- Parents know how to access verified information from the school. ☐
- We integrate critical source evaluation into multiple subjects. ☐
- I model responsible digital communication in my own leadership role. ☐

Recommended Reading and Resources

- UNESCO: media and Information Literacy Curriculum for Teachers.[2]
- News Literacy Project: free teaching resources and guides.[3]
- Full Fact (UK) (https://fullfact.org/), Snopes (US) (https://www.snopes.com/), EU vs Disinfo (Europe) (https://euvsdisinfo.eu/): Reliable fact-checking organisations.
- DROG's "Bad News" Game: an interactive resource that helps players understand disinformation strategies (https://www.getbadnews.com/en/play) available in many languages.

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

3 https://newslit.org/educators/

Conclusion

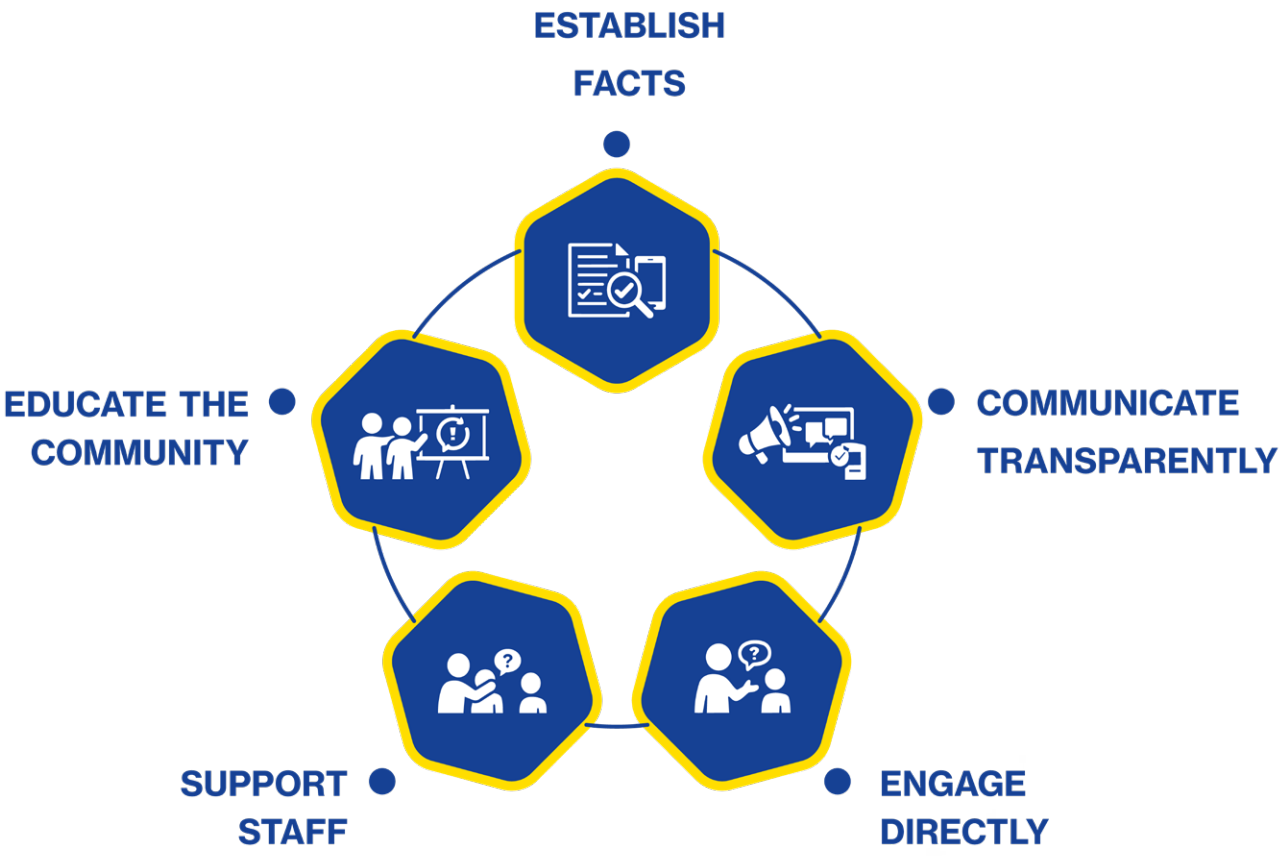
Disinformation, misinformation, and fake news are not external issues “out there” in the wider world. They reach directly into school corridors, classrooms, and communities. For school leaders, the task is twofold: to protect the school community from harm and to empower students and staff with lifelong skills for navigating digital environments.

This requires leaders to:

- Strengthen their own skills in recognising and responding to false information.
- Equip teachers with training, tools, and confidence. Communicate transparently with parents and communities.
- Build resilience so that misinformation becomes an opportunity for growth, not crisis.

By taking these steps, school leaders not only address immediate risks but also fulfil a deeper educational mission: preparing young people to live as informed, critical, and responsible citizens in a world where truth itself is often contested.

STEPS FOR LEADERS IN A CRISIS SITUATION



CHAPTER 3

RESILIENCE BUILDING

Why Resilience Matters in the Digital Age

Resilience is often described as the capacity to recover quickly from challenges or setbacks. In the digital age, resilience also includes the ability to withstand harmful content, online manipulation, and the fast-moving pressures of social media. For schools, resilience is not only an individual trait but also a collective capacity.

- For students, resilience means the ability to cope with exposure to harmful online trends, cyberbullying, or false information without long-term damage to wellbeing.
- For teachers, resilience means the capacity to adapt to new challenges, including online harassment, rapid technological changes, or misinformation crises in their classrooms.
- For school leaders, resilience involves managing institutional challenges with calmness and foresight – ensuring that when problems arise, the school community is equipped to respond constructively rather than reactively.

The DRONE research underscores that resilience is not innate. It is a learnable competence that can be strengthened through deliberate school policies, leader modelling, and collective practice.

Building Your Own Resilience as a School Leader

Leadership in a digital age is demanding. Disinformation, cyber incidents, and community conflicts can test even the most experienced school leaders. Developing resilience begins with self-awareness and personal strategies.

Self-Assessment Questions for Leaders

1. Do I remain calm under pressure, or do I feel overwhelmed when digital crises emerge?
2. Am I confident in separating fact from emotion when responding to online rumours?
3. Do I have personal strategies (e.g., peer support networks, reflection practices) to manage stress?
4. Do I model constructive responses when faced with misinformation or online hostility?

Personal Resilience Practices

- Establish information boundaries: Avoid reacting immediately to every message or rumour. Take time to verify and consult before responding.
- Use professional networks: Build peer support among other school leaders to share strategies and experiences.
- Prioritise wellbeing: Ensure you have routines (exercise, rest, mindfulness) that maintain mental balance. A stressed leader struggles to make calm decisions.
- Model resilience: Students and staff notice how leaders react. Your calm, measured response sets a tone for the entire community.

Supporting Teachers in Building Resilience

Teachers are at the front line of digital challenges. They may be exposed to cyberbullying from students, online harassment from parents, or overwhelming demands to manage new technologies. Leaders must actively support staff in building resilience.

Leadership Actions

1. Professional Development: Offer training in coping strategies for digital stress, including managing hostile messages and protecting professional boundaries online.

2. Clear Policies: Ensure staff know what steps to take if they are targeted online (e.g., reporting to leadership, documenting incidents, involving authorities if necessary).

3. Workload Balance: Digital initiatives should not overburden staff. Leaders should ensure that technology enhances learning rather than creating unnecessary administrative stress.

4. Wellbeing Programmes: Embed resilience into staff wellbeing programmes, emphasising that seeking help is a strength, not a weakness.

Check how resilience, mental health, and online safety are defined in national education or childwellbeing policies and use the same terminology in your school documents. This shared language helps external services and authorities collaborate smoothly with your school when problems arise.

Example: Teacher Harassment Online

At one school, a teacher was mocked anonymously on a social media account run by students. The headteacher acted quickly, reassuring the teacher that leadership took the issue seriously, involving parents, and working with the platform to remove the content. The teacher received emotional support from colleagues and guidance on protecting their professional digital presence. The incident reinforced the importance of leaders creating a culture of zero tolerance for online harassment.

Building Resilience Among Students

Students are often the most vulnerable to digital pressures. They may encounter false narratives, harmful trends, or cyberbullying. Leaders play a key role in creating environments where resilience is taught, practised, and reinforced.

Strategies for Student Resilience

- Embed digital resilience into the curriculum: Lessons should include coping strategies, not just warnings about risks.
- Create safe reporting mechanisms: Ensure students know they can report harmful online experiences without fear of punishment.
- Promote peer support: Encourage student leaders or mentors to support peers facing digital challenges.
- Focus on emotional skills: Help students understand emotional triggers, manage stress, and think before reacting online.

Practical Example: Student Workshops

One school introduced a workshop called “Pause Before You Post,” teaching students how to slow down, reflect, and verify before responding to provocative online content. The workshop used role-play scenarios and group discussions. Students later reported feeling more confident in resisting peer pressure to share harmful or false content.

When Things Go Wrong – From Challenges to Crises

Resilience is tested most in moments of crisis. Schools may face situations such as:

- A viral harmful challenge encouraging risky behaviour.
- Online bullying targeting students or staff.
- Community anger fuelled by disinformation.
- A data breach exposing student information.

Leader's Response Framework: The "4 Cs"

1. Calm: Do not escalate panic. Show composure and measured decision-making.
2. Clarity: Communicate verified information transparently.
3. Care: Prioritise the wellbeing of students and staff, offering counselling or practical support where needed.
4. Community: Involve parents, local authorities, and external experts to create a united response.

Example: Viral Online Challenge

At a large secondary school, students became anxious about a viral "dangerous challenge" circulating on TikTok. Rumours spread that some students had attempted it. The headteacher convened a crisis team, verified no students had been directly involved, and issued a clear statement to parents explaining the situation. In assemblies, students were taught how viral hoaxes spread and how to resist peer pressure. The school provided counselling to those who felt distressed. The proactive response prevented hysteria and strengthened the community's trust in leadership.

Creating a Resilient School Culture

Resilience is not only about individuals – it must be embedded in the school's systems and culture.

Key Actions for Leaders

- Policy Integration: Make resilience part of safeguarding, behaviour, and wellbeing policies.
- Regular Drills: Just as schools practise fire drills, consider "digital incident drills" where staff and students rehearse responses to misinformation or cyberbullying.
- Recognition and Rewards: Celebrate examples of resilience among staff and students (e.g., recognising a student who calmly resisted peer pressure to share harmful content).
- Community Involvement: Partner with parents, local organisations, and mental health services to create a broader support network.

Practical Tools for School Leaders

Resilience Checklist for Leaders

- I have strategies to manage my own stress during digital crises. ☐
- Staff have access to clear policies and training on resilience. ☐
- Students are taught emotional and digital resilience skills in lessons. ☐
- We have safe reporting systems for digital harms. ☐
- Our crisis communication plan prioritises calm, clarity, care, and community. ☐
- Parents are engaged as equal partners in supporting resilience. ☐

Recommended Resources

- UK Safer Internet Centre: Resources on resilience and online safety.[4]
- UNICEF: Guidance on digital wellbeing for children and schools.[5]
- Ditch the Label: Organisation offering resources on online bullying and resilience.[6]
- SAILS project tools: Practical exercises for evaluating emotional responses to online content.

4 https://saferinternet.org.uk/?s=Resources%20on%20resilience%20and%20online%20safety.&post_type=resource

5 https://www.unicef.org/eu/media/2586/file/Digital%20technologies%20policy%20brief.pdf

6 https://ditchthelabel.org/

Conclusion

Resilience in schools is not about preventing every crisis or shielding students from all harm. It is about building the capacity to respond constructively when challenges arise. For school leaders, this involves:

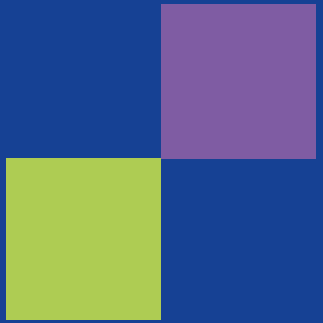
- Developing their own resilience practices.
- Supporting teachers in coping with digital stress and harassment.
- Embedding resilience-building for students into the curriculum and culture.
- Leading crisis responses that model calmness, clarity, care, and community.

When schools develop resilience as a shared competence, they are not only safer and more prepared but also more confident. Leaders who prioritise resilience prepare their schools for the uncertainties of a fast-changing digital world – and equip students with the lifelong ability to face challenges with strength and critical awareness.

Leader's Response Framework: The "4 Cs"

CHAPTER 4

PROBLEM-SOLVING



Why Problem-Solving Matters in the Digital Age

Schools have always faced challenges, from playground disputes to curriculum changes. But in the digital age, problems often arise suddenly, spread quickly, and have unpredictable impacts. A single misleading post can spark widespread confusion. A software failure can disrupt learning for hundreds of students. A cyberbullying incident can escalate into a crisis involving parents, media, and authorities.

Effective problem-solving is therefore not just a useful leadership trait. It is a core competence for school leaders who must balance competing demands, resolve conflicts, and guide staff and students through complex digital dilemmas.

The DRONE research emphasises that digital problem-solving requires three key capacities:

1. Critical thinking – identifying the real issue beneath the noise.
2. Creativity – generating multiple solutions, not just quick fixes.
3. Confidence – acting decisively, even under pressure.

Developing Problem-Solving Skills as a School Leader

Before guiding teachers or students, leaders must strengthen their own problem-solving abilities.

A Reflective Framework: The "STOP" Method

- S – Slow Down: Resist the urge to react impulsively to online rumours or digital incidents.
- T – Think Clearly: Define the actual problem. Is it a misinformation issue, a technical fault, or a relationship breakdown?
- O – Options: Brainstorm possible solutions. Involve staff when appropriate.
- P – Plan and Proceed: Choose the most effective option, communicate it clearly, and follow through.

Self-Assessment Questions for Leaders

1. Do I tend to act quickly without verifying information first?
2. Am I comfortable seeking advice from others, or do I try to solve problems alone?
3. Do I encourage creative approaches, or do I stick rigidly to standard procedures?
4. Can I remain calm when parents, staff, or students pressure me for immediate answers?

By reflecting on these questions, leaders can identify their strengths and weaknesses in digital problem-solving.

Supporting Teachers in Problem-Solving and Decision-Making

Teachers face frequent digital dilemmas:

- A student cites false information in an assignment.
- An online group chat turns toxic.
- A parent emails demanding immediate answers about a rumour.

Without support, teachers may feel overwhelmed or inconsistent in their responses. Leaders can strengthen teachers' problem-solving capacity in several ways:

Leadership Actions

1. Professional Training: Offer workshops on digital dilemmas, using real-life scenarios and role-play.

2. Shared Protocols: Develop school-wide guidelines (e.g., how to escalate misinformation, cyberbullying, or online harassment).

3. Empowerment: Give teachers autonomy to make decisions within clear frameworks, so they feel confident handling smaller issues without always seeking leadership intervention.

4. Peer Learning: Create spaces where teachers share "problem-solving stories" – what they faced, how they responded, and what they learned.

Review your crisisresponse procedures against national and municipal emergency or riskmanagement regulations for schools. Explicitly citing these policies in staff guidance reassures your community that decisions in digital crises rest on a recognised legal and professional basis.

Example: Staff Scenario Training

A school head introduced monthly "digital dilemmas" at staff meetings. One month, teachers role-played responding to a parent who forwarded a conspiracy-laden article about the school. Another month, they discussed a fake student account on Instagram. Teachers reported feeling far more prepared for real-life issues after practising responses in a safe environment.

Building a Problem-Solving Culture for Students

Students need explicit guidance in problem-solving. Online life presents them with daily choices: whether to share content, respond to bullying, or believe a rumour. Without structured practice, they may rely on emotion or peer influence instead of critical reasoning.

Strategies for Student Problem-Solving

- Inquiry-Based Learning: Pose open-ended questions that require students to evaluate digital content and propose solutions.
- Group Challenges: Create classroom activities where students solve real-world digital problems collaboratively.
- Decision-Making Tools: Teach simple frameworks like “Stop, Think, Check, Act” for evaluating online choices.
- Reflective Practice: After digital incidents, guide students to reflect on what went wrong, what choices were available, and what they might do differently next time.

Example: Digital Decision-Making Project

A middle school introduced a project where students investigated viral online challenges. In groups, they researched how the challenge spread, why people participated, and what risks were involved. Students then created presentations on safer alternatives. This turned a dangerous trend into a structured learning exercise in digital problem-solving.

When Things Go Wrong – From Challenges to Crises

Even with strong systems, schools will face unexpected crises. The key is not to avoid every problem but to respond constructively when they escalate.

Common Digital Crises

- A hacked school account shares inappropriate content.
- A viral rumour claims the school is hiding a serious safety issue.
- Cyberbullying escalates into threats.
- A technical failure during exams disrupts assessment.

Crisis Response Framework for Leaders

1. Identify the Core Issue: Strip away noise and emotion to pinpoint the actual problem.
2. Gather Key People: Involve relevant staff (ICT manager, safeguarding lead, communications officer).
3. Decide Quickly but Wisely: Weigh risks and choose the least harmful option.
4. Communicate Clearly: Share updates with staff, students, and parents in accessible language.
5. Reflect and Review: After resolution, analyse what worked and what can be improved.

Case Study: "The Hacked Account"

At a secondary school, the official social media account was hacked and used to post offensive content. Within an hour, screenshots circulated among parents and students.

Leadership Response

- The headteacher immediately contacted the ICT team to secure the account and remove posts.
- A holding statement was issued to parents explaining that the account was compromised and being restored.
- Police and the platform provider were contacted.
- The incident was later used in assemblies to teach students about password security and digital responsibility.

Outcome

Although initially damaging, the transparent and rapid response reassured parents, restored trust, and turned the crisis into a learning opportunity.

Creating a Problem-Solving School Culture

Problem-solving should not be limited to crises. A resilient school fosters a culture where challenges are seen as opportunities for growth.

Key Actions for Leaders

- Model Openness: Admit when you don't have an immediate solution, and show how you seek one.
- Celebrate Problem-Solvers: Recognise staff and students who demonstrate creative solutions to digital challenges.
- Integrate Across Subjects: Encourage teachers to design lessons that involve evaluating dilemmas and proposing solutions.
- Link to Citizenship Education: Position problem-solving as part of preparing students for democratic, responsible participation in society.

KEY PROBLEM-SOLVING ACTIONS

Practical Tools for School Leaders

Problem-Solving for Leaders

- I apply structured frameworks (e.g., STOP) when tackling digital dilemmas. ☐
- Teachers in my school are trained in consistent problem-solving strategies. ☐
- Students are taught decision-making tools for digital contexts. ☐
- We have clear protocols for responding to digital crises. ☐
- Parents are included in communication during crises as equal partners. ☐
- We reflect on problems after resolution to learn for the future. ☐

Recommended Resources

- OECD Skills Outlook: Research on problem-solving in digital societies.[7]
- Common Sense Education: Lesson plans on digital decision-making.[8]
- SAILS Project Tools: Scenario-based exercises for classroom and staff training.
- MindTools Problem-Solving Frameworks: Adaptable strategies for leadership contexts.[9]

7 https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/11/oecd-skills-outlook-2023_df859811/27452f29-en.pdf

8 https://www.commonsense.org/education/digital-citizenship

9 https://www.mindtools.com/cx4ems0/problem-solving

Conclusion

Problem-solving in schools is no longer just about day-to-day management. In a digital world, leaders must be prepared for sudden misinformation crises, technical failures, and online conflicts that can impact students, staff, and the wider community.

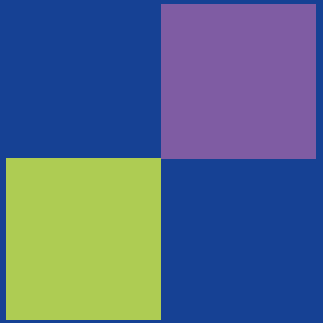
Effective problem-solving involves:

- Developing leaders' own critical, creative, and confident approaches.
- Equipping teachers with frameworks and shared protocols.
- Embedding decision-making skills in student learning.
- Responding to crises with calmness, clarity, and constructive action.

When school leaders champion problem-solving as a whole-school culture, they prepare their communities not only to survive digital challenges but to grow stronger from them.

CHAPTER 5

CRITICAL THINKING



Why Critical Thinking Matters in Schools

Critical thinking is the ability to question, analyse, and evaluate information rather than accepting it at face value. In the digital world, where every student and teacher is exposed daily to thousands of posts, images, and videos, this skill is not optional – it is essential.

For schools, critical thinking is more than an academic skill. It is a foundation for digital resilience, responsible citizenship, and informed decision-making. Without it:

- Students may accept conspiracy theories or harmful online content uncritically.
- Teachers may share unverified information with classes, unintentionally spreading misinformation.
- Parents may lose trust in schools if leaders cannot demonstrate transparent, critical engagement with rumours or policies.

For school leaders, the challenge is twofold: to develop their own critical thinking skills as role models and to create a school culture where questioning and evidence-based reasoning are encouraged.

Developing Leaders' Critical Thinking Skills

Before fostering critical thinking among staff and students, school leaders must strengthen their own capacity. A leader who reacts impulsively to online rumours or makes decisions based on incomplete evidence undermines the culture they are trying to build.

Key Reflective Questions for Leaders

1. When I receive new information, do I ask: Who produced this and why?
2. Do I seek multiple perspectives before making decisions?
3. Do I check for unconscious bias in my own assumptions?
4. Do I model transparency by explaining my reasoning to staff and parents?

Practical Strategies for Leaders

- Pause Before Reacting: Train yourself to verify before responding to online controversies or parent complaints.
- Use Critical Frameworks: Apply tools such as the "5 Ws" (Who, What, When, Where, Why) when reviewing information.
- Engage with Contrasting Views: Read diverse sources to avoid echo chambers, especially on controversial issues.
- Share Your Thinking Process: In meetings, explain not only your decision but how you arrived at it, modelling critical engagement for others.

Fostering Critical Thinking Across the School

A culture of critical thinking cannot be left to chance – it must be deliberately embedded.

Leadership Actions

1. Curriculum Integration: Ensure critical thinking is not confined to one subject (such as ICT or citizenship) but woven across science, history, literature, and the arts.
2. Assessment Models: Reward students for asking questions and challenging assumptions, not just for giving the "right" answer.
3. Staff Collaboration: Encourage teachers to share how they integrate critical questioning into their lessons.
4. Safe Environment: Create a climate where students feel comfortable asking difficult questions without fear of ridicule or punishment.

Where national curricula or competence frameworks describe critical thinking and media literacy, use those references when framing your school's aims. Linking classroom practice to these policy expectations can also strengthen your case when requesting training or resources.

In line with the **HEADstart #4 card**, critical thinking activities should always be grounded in a clearly articulated value framework that emphasises human dignity, equity, and respectful dialogue. Making these values visible in policies and classroom charters helps students understand why certain kinds of online behaviour and content are ethically unacceptable.

Example: Embedding Critical Thinking in History

Instead of simply memorising historical facts, students are encouraged to compare how different sources present the same event. Leaders supported teachers by providing a cross-subject toolkit on source evaluation. This helped normalise questioning as a valued skill, not a sign of defiance.

Supporting Teachers in Developing Critical Thinking

Teachers themselves need confidence in their critical skills to effectively support students. Many feel under pressure to "cover content" quickly and may neglect time for deeper questioning. Leaders can address this by:

- Professional Development: Provide training on questioning techniques and digital source analysis.
- Resource Sharing: Offer templates, checklists, and classroom activities focused on evaluating information.
- Encouragement: Recognise and celebrate teachers who successfully foster critical discussions, even when the outcome is complex rather than neat.
- Modelling: Show teachers that it is acceptable not to have all the answers – what matters is the willingness to think critically alongside students.

Example: Peer-Led Learning

At one school, teachers created a "critical thinking circle" where staff observed each other's lessons, focusing specifically on questioning strategies. Leaders supported this by allocating meeting time and recognising it in professional reviews. Teachers reported that their own confidence in handling student questions improved significantly.

Supporting Students in Critical Engagement with Digital Content

Students are often eager consumers of digital media but less skilled at evaluating it. Leaders must ensure that classrooms become places where students are taught to slow down, reflect, and question.

Strategies for Students

- Practical Exercises: Compare two news stories on the same event and discuss which is more credible and why.
- Guided Questions: Teach students simple prompts such as “Who said this?” and “What evidence supports it?”
- Role-Play: Ask students to act as “fact-checkers” in classroom debates.
- Project Work: Assign research projects that require evaluating sources, not just collecting information.

Example: Student-Led Fact-Checking Club

One secondary school created a student club where participants fact-checked viral rumours and produced short reports for peers. With leader endorsement, the club became a trusted voice among students and helped normalise critical engagement with online content.

When Things Go Wrong – From Challenges to Crises

Critical thinking is most valuable in moments of confusion or tension, when misinformation or rumours spread rapidly. Leaders need clear approaches to maintain credibility and prevent panic.

Common Scenarios

- A rumour spreads that a teacher has been dismissed for misconduct.
- Parents forward conspiracy theories about a new school policy.
- Students circulate doctored images suggesting dangerous incidents in the school.

Leader's Response Strategy

1. Verify: Establish the facts quickly through trusted channels.
2. Acknowledge Uncertainty: If you don't yet know the full truth, say so honestly.
3. Communicate Clearly: Provide updates in plain language, free from jargon or defensive tone.
4. Educate Through Crisis: Use the incident as a real-world lesson in critical thinking for staff, students, and parents.

Case Study: "The Doctored Image"

A photo appeared online showing apparent vandalism in the school cafeteria, captioned with claims that students were "out of control." Parents began sharing it in local community groups.

Leadership Response

- The school head verified CCTV footage, which showed that the image had been digitally altered.
- A clear statement was issued to parents explaining the manipulation and reassuring them about student behaviour.
- In assemblies, the incident was used to teach students about image editing and the importance of questioning online visuals.

Outcome

The school not only restored parental trust but also used the event as a powerful teaching moment in critical media literacy.

Creating a School Culture of Critical Thinking

Critical thinking cannot be imposed – it must be encouraged through trust, openness, and consistent reinforcement. Leaders play a pivotal role in embedding it into the school ethos.

Key Actions for Leaders

- Promote Curiosity: Reward students who ask questions, not just those who provide answers.
- Encourage Staff Reflection: Ask teachers to share how they model questioning in lessons.
- Communicate Transparently: Demonstrate critical thinking in leadership communications, especially during crises.
- Engage Parents: Offer workshops for families on evaluating information, ensuring critical thinking extends beyond the school gates.

Practical Tools for School Leaders

Critical Thinking Checklist for Leaders

- I model critical questioning in my leadership communications. ☐
- Teachers have access to training and resources for fostering critical thinking. ☐
- Students are explicitly taught evaluation strategies across subjects. ☐
- Our school recognises and rewards curiosity and questioning. ☐
- We use misinformation incidents as learning opportunities. ☐
- Parents are included in critical thinking initiatives as assets and equal partners. ☐

Recommended Resources

- UNESCO Media and Information Literacy Curriculum[10]
- News Literacy Project (US) – classroom-ready resources[11]
- Full Fact (UK) – tools for verifying claims[12]
- SAILS Project Exercises – practical critical thinking scenarios for schools[13]

10 https://www.unesco.org/mil4teachers/en/curriculum

11 https://newslit.org/educators/?gad_source=1&gad_campaignid=13609440607&gbraid=0AAAADrR_oy_4kH3dk6h9LRxVselZ2rKy&gclid=CjwKCAjwk7DFBhBAEiwAeYbJsb7KO8oXhyt_hdKVQRH5HYtgKQHwzTiJt_y6fJ5TGRqYbiodDnpb4hoCGGMQAvD_BwE

12 https://fullfact.org/

13 https://sails.deusto.es/

Conclusion

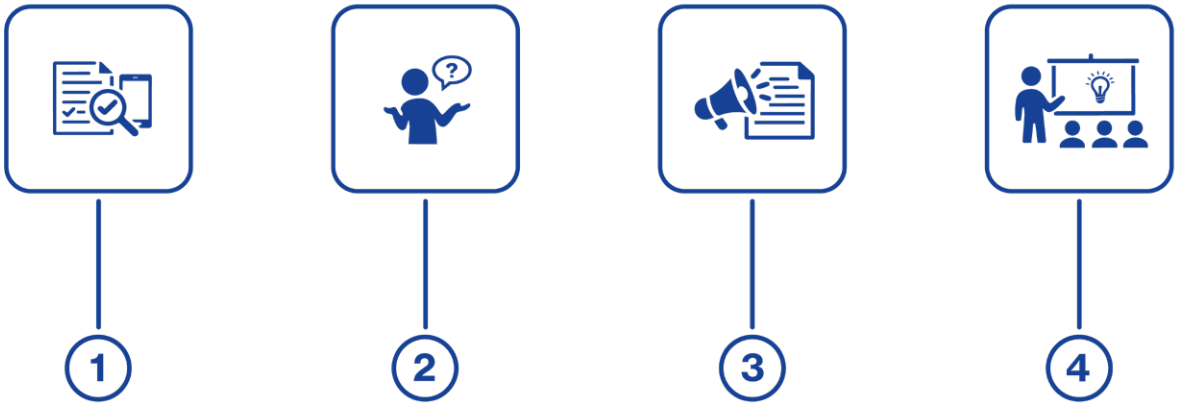
Critical thinking is the cornerstone of digital literacy. For school leaders, it is both a personal skill to practise and a cultural value to embed. By:

- Strengthening their own questioning abilities.
- Supporting teachers with training and tools.
- Equipping students with simple evaluation strategies.
- Communicating transparently with parents and communities.

School leaders can transform schools into spaces where truth, curiosity, and evidence are valued.

In an age of misinformation, a school that fosters critical thinking is not just teaching students to succeed academically. It is preparing them to thrive as thoughtful, responsible citizens in a world where information is abundant, but truth must be actively pursued.

LEADER'S RESPONSE STRATEGY TO CRITICAL-THINKING PROBLEMS



1. VERIFY
2. ACKNOWLEDGE UNCERTAINTY
3. COMMUNICATE CLEARLY
4. EDUCATE THROUGH CRISIS

CHAPTER 6

BULLYING AND CYBERBULLYING

Why Bullying Deserves Leadership Attention

Bullying is not new, but digital technologies have magnified its reach and impact. A cruel comment that once stayed in the playground can now be shared with hundreds of people in seconds. Photos or videos can be altered and spread widely, making humiliation public and long-lasting. For schools, bullying – especially cyberbullying – is one of the most pressing challenges to student safety and wellbeing.

The DRONE research highlights a critical but often overlooked reality: although peer-to-peer bullying is the most visible form, students are sometimes bullied by teachers or family members. These forms of abuse are often hidden, under-reported, and deeply damaging. School leaders must acknowledge them, create safe reporting systems, and act decisively.

Understanding Bullying and Cyberbullying

Bullying is repeated, intentional behaviour that causes harm, imbalance of power, and distress. Cyberbullying refers to bullying that occurs through digital platforms, including:

- Hurtful messages, memes, or posts.
- Fake accounts impersonating a student.
- Exclusion from online groups.
- Spreading rumours or images digitally.

Key Features of Cyberbullying

- 24/7 Reach: Victims can feel there is no escape.
- Amplification: Online content can spread quickly and widely.
- Anonymity: Bullies may hide behind fake profiles.
- Persistence: Harmful content can remain accessible indefinitely.

Bullying by Teachers: The “Hidden” Problem

It is uncomfortable but necessary to acknowledge that some students are bullied by those entrusted with their care. Teacher bullying online (but also offline) may include:

- Humiliating or ridiculing a student publicly.
- Unfairly targeting a student with harsh discipline.
- Making discriminatory or demeaning remarks.
- Using sarcasm or authority to intimidate rather than to guide.

Why It Is Often Missed

- Students may fear retaliation or believe no one will listen.
- Colleagues may normalise harsh behaviour as “tough teaching.”
- Parents may hesitate to challenge authority figures.

Leadership Responsibilities

- Establish a zero-tolerance policy: Bullying is unacceptable regardless of who perpetrates it.
- Provide confidential reporting systems for students and parents.
- Ensure independent investigations of allegations involving staff.
- Promote a culture where respectful, supportive teacher–student relationships are the norm.

Ensure your anti-bullying and cyberbullying procedures mirror definitions, reporting routes, and thresholds set out in national safeguarding or child protection regulations. Referencing these policies in your school documents helps staff recognise when an incident must be escalated beyond the school.

Following **HEADstart #11**, the school’s code of conduct should state explicitly that legal and ethical expectations about respect, non-discrimination, and privacy apply to all digital interactions. It should clarify which behaviours may constitute harassment, hate speech, or unlawful sharing of images or personal data, and how these will be recorded and escalated.

Bullying by Family Members

While schools cannot control home environments, they must recognise when students are experiencing bullying from parents, siblings, or other carers. Family bullying may include:

- Constant criticism or belittling of the child.
- Digital surveillance or shaming via social media.
- Sibling harassment tolerated or encouraged by parents.

Signs Teachers and Leaders May Notice

- A student is consistently anxious or withdrawn after weekends.
- Sudden reluctance to use digital devices.
- Evidence of family members sharing embarrassing content online.

Leadership Role

- Train staff to recognise warning signs.
- Provide safe, confidential ways for students to disclose concerns.
- Work with safeguarding services to support the child and, where necessary, intervene.

Peer Bullying: Still a Concern

While less frequent than public narratives sometimes suggest, peer bullying remains damaging. It can undermine self-esteem, academic progress, and a sense of belonging. Leaders should treat even small incidents seriously to prevent escalation.

Types of Peer Cyberbullying

- Group exclusion from chats or games.
- “Pile-ons” where multiple students target one peer.
- Sharing embarrassing images or videos without consent.

Supporting Teachers in Handling Bullying

In most cases, cyberbullying does not happen in school, but the effects may be felt in school. If this happens, teachers and school heads may need to collaborate with parents and the students to tackle it.

Teachers are often the first to hear about bullying but may feel ill-equipped to act, especially if it involves digital evidence. Leaders can empower teachers by:

- Providing Clear Procedures: Teachers should know exactly how to report and escalate incidents.
- Training on Digital Evidence: Teachers must understand how to preserve screenshots, messages, or posts appropriately.
- Encouraging Empathy-Based Approaches: Teachers should address both victims and perpetrators with a focus on repair, not just punishment.
- Backing Them Up: Teachers must feel leadership will support them if they take action, even in sensitive cases involving parents or staff.

Supporting Students Experiencing Bullying

School leaders must ensure that students who experience bullying – whether from peers, teachers, or family members – receive immediate and long-term support. It is also important to remember that bullying is a learned behaviour, so most of the perpetrators are also victims or have been exposed to bullying as onlookers. Thus, the bullies also need to be treated carefully, and leadership action should aim at finding the causes of bullying.

Key Actions

- Safe Reporting: Multiple reporting options (digital forms, trusted staff, peer mentors).
- Swift Action: Prompt investigation and communication to demonstrate seriousness.
- Counselling and Support: Access to pastoral care, mentoring, or external services.
- Restorative Practices: Where possible, safe opportunities for resolution and rebuilding trust.

When Things Go Wrong – From Challenges to Crises

Bullying incidents can escalate into crises that affect the entire school community.

Common Crises

- A video of a bullying incident goes viral, attracting media attention.
- A teacher is accused of humiliating students online.
- Parents use social media to attack staff over perceived inaction.

Crisis Leadership Framework

1. Immediate Response: Stop the harm, remove harmful content, and ensure student safety.
2. Transparent Communication: Share verified updates with parents, staff, and students.
3. Protect Privacy: Avoid naming victims or perpetrators publicly.
4. Learn and Prevent: After resolution, review policies and ensure lessons are shared across the school.

CRISIS LEADERSHIP FRAMEWORK IN CASE OF BULLYING OR CYBERBULLYING

1 IMMEDIATE RESPONSE

2 TRANSPARENT COMMUNICATION

3 PROTECT PRIVACY

4 LEARN AND PREVENT

Case Study 1: Teacher Bullying

A Year 8 student reported that a teacher regularly mocked their accent in front of peers. At first, leadership hesitated to act, concerned about reputational harm. Eventually, other students confirmed the behaviour.

Response:

- An external investigator was appointed.
- The teacher was suspended during inquiry.
- Training on unconscious bias and respectful communication was rolled out to all staff.

Outcome:

The case was difficult but essential. By acting decisively, the school reinforced its commitment to student dignity and established stronger safeguarding practices.

Case Study 2: Viral Peer Bullying Video

At a secondary school, a fight in the playground was filmed and shared widely online, captioned to humiliate one student.

Response:

- Leadership worked with social media platforms to remove the video.
- Parents of all involved students were contacted.
- Assemblies addressed digital citizenship and bystander responsibility.
- Counselling was offered to the targeted student.

Outcome:

The school used the incident as a learning moment, reinforcing a culture of care and digital responsibility.

Creating a Bullying-Resistant School Culture

Prevention is more effective than crisis management. Leaders should create a school climate where bullying of any form is unacceptable.

Key Steps

- Policy Clarity: Ensure bullying policies explicitly include teachers and family contexts.
- Regular Training: Refresh all staff annually on recognising and addressing bullying.
- Student Voice: Involve students in shaping anti-bullying strategies.
- Parental Partnerships: Offer parents collaborative workshops with teachers on digital responsibility and family dynamics.
- Visibility of Values: Promote respect, empathy, and inclusion in school communications and events.

Practical Tools for School Leaders

Bullying Checklist for Leaders

- Policies cover teacher and family bullying, not just peer incidents. ☐
- Staff receive annual training on recognising and reporting bullying. ☐
- Students have safe, accessible reporting channels. ☐
- Digital evidence protocols are in place. ☐
- Responses prioritise safety, dignity, and restorative practices. ☐
- Parents are engaged in prevention and response as equal partners. ☐

Recommended Resources

- Anti-Bullying Alliance (UK) – training and tools for schools.[14]
- UNICEF Guidance – bullying and online safety.[15]
- Ditch the Label – resources on peer and digital bullying.[16]
- SAILS Project Tools – checklists for recognising bullying behaviours. (https://library.parenthelp.eu/seafarers-guide/, https://library.parenthelp.eu/captains-handbook-sails-resource-for-school-leaders/)

14 https://anti-bullyingalliance.org.uk/tools-information/free-cpd-online-training

15 https://www.unicef.org/stories/how-to-stop-cyberbullying#:~:text=If%20you're%20experiencing%20bullying,within%20Facebook%2C%20Instagram%20or%20Threads.

16 https://ditchthelabel.org/

Conclusion

Bullying – whether by peers, teachers, or family members – is a profound violation of trust and safety. School leaders must:

- Confront uncomfortable realities, including adult-to-child bullying.
- Provide teachers with training and support to act confidently.
- Ensure students feel heard, protected, and supported.
- Respond to crises with clarity, compassion, and decisive action.

By creating a culture where respect is non-negotiable and bullying is never tolerated, leaders can transform schools into places of safety and dignity. In doing so, they not only protect individual students but also strengthen the entire community.

CHAPTER 7

CYBERSECURITY

Why Cybersecurity Is a Leadership Issue

Cybersecurity in schools is not just a technical matter for IT staff. It is a strategic leadership responsibility. A single breach – whether a hacked email account, a stolen password, or leaked student data – can undermine parent trust, damage staff morale, and even put children at physical risk.

Digital infrastructure is now as essential as water and electricity. School leaders must treat cybersecurity with the same seriousness, ensuring that systems are protected, staff are trained, and students are safe.

The DRONE research shows that many leaders underestimate cybersecurity until a crisis occurs. Too often, security is viewed as a "back-end issue," when in reality, it requires whole-school policies, culture, and vigilance.

Cybersecurity in the School Setting

Schools are attractive targets for cyberattacks because they hold sensitive data:

- Student personal records, including health and safeguarding information.
- Staff employment and payroll details.
- Examination results and assessment data.
- Login credentials for multiple online learning systems.

Common threats include:

- Phishing emails tricking staff into revealing passwords.
- Ransomware attacks locking files until a payment is made.
- Data breaches exposing student and staff information.
- Insecure devices connecting to school networks without safeguards.

Developing Leaders' Cybersecurity Competence

Before protecting others, leaders must develop their own digital security skills. If leaders themselves fall victim to phishing scams or weak password practices, they cannot credibly champion a culture of cybersecurity.

Self-Check Questions

1. Do I use strong, unique passwords (or a password manager) for school accounts?
2. Am I confident identifying suspicious emails or links?
3. Do I keep my own devices updated with the latest software and security patches?
4. Am I aware of the school's incident response plan for data breaches?
5. Do I model safe practices when sharing information with parents and staff?

If the answer to any of these is "no," the leader must prioritise personal cybersecurity training.

Supporting Teachers in Cybersecurity Awareness

Teachers often manage sensitive information: grades, safeguarding reports, personal communication with parents. Without training, they may inadvertently expose data or fall victim to scams.

Leadership Actions

- Mandatory Training: Provide annual sessions on phishing awareness, password hygiene, and data protection.
- Practical Simulations: Use mock phishing emails to test awareness and encourage discussion.
- Clear Protocols: Teachers should know exactly how to report suspicious emails or potential breaches.
- Support, Not Blame: Frame training as empowerment, not punishment – mistakes should become learning opportunities.

Align your school's cybersecurity rules with national or regional data protection legislation and any education sector security standards. Clearly signposting these references in staff handbooks reminds everyone that digital safety is both a legal obligation and a pedagogical priority.

HEADstart #20 reminds leaders that cybersecurity is inseparable from legal compliance with GDPR and children's data protection rights. School leaders should therefore know their data protection officer, understand national reporting duties, and ensure that every technical measure is backed by lawful and transparent data handling practices.

Supporting Students in Cybersecurity

Students, too, need guidance in protecting themselves online. While IT classes may cover some basics, school leaders should ensure cybersecurity is embedded in broader digital literacy efforts.

Strategies for Students

- Password Practices: Teach students to create strong, memorable passphrases.
- Privacy Awareness: Encourage them to think critically before sharing personal data online.
- Device Security: Promote safe use of school and personal devices (updates, secure logins).
- Peer Learning: Create opportunities for older students to mentor younger peers on cybersecurity.

When Things Go Wrong – From Challenges to Crises

Despite precautions, schools may face cybersecurity incidents.

Common Crises

- A ransomware attack encrypts school files, demanding payment.
- A staff member clicks on a phishing email, exposing login credentials.
- A parent group email leaks personal student information.
- A hacked social media account spreads false messages on behalf of the school.

Crisis Management Framework for Leaders

1. Contain the Incident: Disconnect compromised systems immediately.
2. Inform Key People: Alert IT staff, relevant authorities, and data protection officers.
3. Communicate Carefully: Share clear, factual updates with staff and parents. Avoid speculation.
4. Support Affected Individuals: If data is leaked, provide guidance on monitoring and protection.
5. Learn and Improve: Review the incident to strengthen policies and training.

Case Study 1: The Phishing Email

A secondary school office manager received an email appearing to come from the school head, requesting urgent transfer of funds for "equipment." The manager nearly complied but paused to check directly with the headteacher, preventing loss.

Leadership Lessons:

- Regular training had raised awareness, enabling the pause.
- Open communication culture encouraged verification rather than blind compliance.
- After the incident, the school updated its financial procedures to require multi-person authorisation.

Case Study 2: The Ransomware Attack

A primary school's systems were locked by ransomware, making attendance, assessment, and communication systems inaccessible. Hackers demanded payment.

Response:

- The school contacted local authorities and IT specialists immediately.
- Backups were restored, avoiding ransom payment.
- Parents were informed through printed letters and community noticeboards.
- Training on ransomware was introduced for all staff.

Outcome:

The crisis highlighted the importance of offline backups and transparent communication. Parent trust increased because of honest leadership.

Building a Cybersecurity Culture

Cybersecurity must be more than rules – it must become a shared culture across the school.

Steps for Leaders

- Set the Tone: Talk about cybersecurity regularly in staff meetings and newsletters.
- Reward Vigilance: Acknowledge staff or students who report suspicious activity.
- Normalise Caution: Encourage a “better safe than sorry” approach to unknown links or attachments.
- Work with Parents: Provide teachers and parent workshops on home cybersecurity, ensuring consistency between school and home environments.

Practical Tools for Leaders

Cybersecurity Checklist for School Leaders

- I use strong, unique passwords and encourage staff to do the same. ☐
- Staff receive annual cybersecurity training with simulations. ☐
- We have a clear, tested incident response plan. ☐
- Sensitive data is encrypted and regularly backed up. ☐
- Students are taught age-appropriate cybersecurity practices. ☐
- Parents are engaged in home cybersecurity awareness. ☐
- Relationships with technology providers include clear security expectations.

Recommended Resources

- National Cybersecurity Centre (NCSC, UK) – guidance for schools.[17]
- EU Kids Online Project – research and resources on children's digital safety.[18]
- Common Sense Education – classroom resources on student cybersecurity.[19]
- SAILS Project Tools – checklists and practical exercises. (https://library.parenthelp.eu/captains-handbook-sails-resource-for-school-leaders/)

Drawing on **HEADstarts #20** and **#21**, the cybersecurity checklist should ask whether all data flows, thirdparty tools, and storage locations have been mapped and assessed against GDPR and UNCRC principles. It should also verify that consent procedures, dataminimisation, retention rul, and pupils' rights of access or erasure are clearly defined and communicated

17 https://www.ncsc.gov.uk/section/education-skills/schools

18 https://eucpn.org/document/eu-kids-online-final-report

19 https://www.commonsense.org/education/articles/teachers-essential-guide-to-cybersecurity

Conclusion

Cybersecurity is not optional or technical jargon – it is about safeguarding the trust, safety, and integrity of the entire school community.

For school leaders, effective cybersecurity means:

- Strengthening their own digital security practices.
- Ensuring staff are confident and supported.
- Embedding cybersecurity into student learning.
- Responding swiftly and transparently when incidents occur.

A secure school is one where students' data, teachers' work, and community trust are all protected. Leaders who treat cybersecurity as a cultural priority, not just an IT issue, will build resilience against threats and prepare students for safe digital futures.

CHAPTER 8

BUILDING ALLIANCES

Why Building Alliances Matters

Schools do not exist in isolation. They interact daily with technology providers, social media platforms, government agencies, parents, community organisations, and industry partners. These relationships can provide valuable resources, innovative tools, and new opportunities for students. But they can also expose schools to imbalanced contracts, data exploitation, and ethical dilemmas.

The DRONE research highlights that school leaders often enter partnerships without fully understanding the long-term consequences. Decisions about software licences, data-sharing agreements, or corporate sponsorships can shape how students learn, how staff work, and how family trust is maintained.

School leaders must therefore become critical gatekeepers: welcoming positive alliances, rejecting exploitative ones, and ensuring every relationship supports the school's mission of safeguarding and educating young people.

Evaluating Digital Relationships with Companies and Entities

Every contract, whether with a major tech provider or a small educational start-up, carries risks.

Key Questions for Leaders Before Signing Any Agreement

1. What data will be collected? Student and staff personal information, behavioural data, or usage patterns?

2. Who owns the data? Will the school retain ownership, or can the company use it for commercial purposes?

3. How transparent is the company? Do they provide clear, plain-language explanations of terms?

4. What happens if the contract ends? Will data be deleted, transferred, or sold?

5. Does the partnership align with school values? Does it promote equity, safety, and learning – or primarily serve corporate interests?

Practical Steps

- Involve both legal advisors and safeguarding staff before signing.
- Seek out independent reviews of the product or service.
- Pilot new tools on a small scale before rolling out school-wide.
- Engage parents in discussions about data use and new platforms.

When evaluating contracts or partnerships, check them against national regulations on data protection, public procurement, and commercial activities in schools. Noting these policy references in partnership documentation strengthens your position if you need to renegotiate or terminate an agreement.

Promoting Ethical Digital Relationships

Building alliances is not only about protecting the school from harm. Done well, partnerships can enrich learning and create meaningful opportunities.

Examples of Positive Alliances

- Collaborations with universities for digital literacy research.
- Partnerships with local businesses offering safe online internships.
- Work with non-profits on student digital resilience training.
- Community-led projects on cyber safety awareness.

Leadership Role

- Set the ethical standard: Make clear that the school will not compromise student privacy for financial gain.
- Model transparency: Share contracts, agreements, and decisions openly with staff and parents.
- Prioritise equity: Ensure that digital tools are accessible to all students, not just those with resources at home.

When Things Go Wrong – From Challenges to Crises

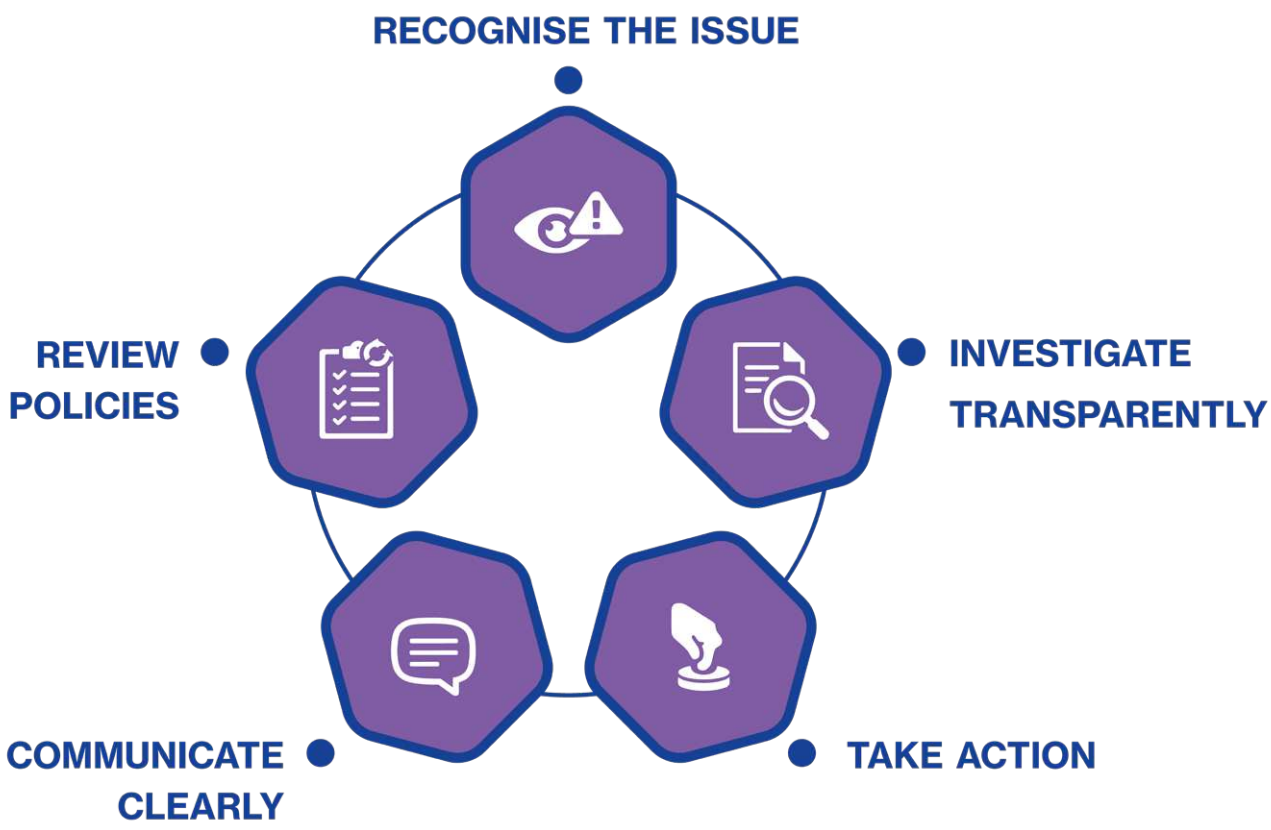
Even well-intentioned partnerships can go wrong. Leaders must be ready to respond when alliances threaten school values or student safety.

Common Scenarios

- A company uses student data for advertising without consent.
- A sponsor pressures the school to promote products in return for funding.
- Parents discover that their child's online activity in a school platform has been tracked for commercial use.

Crisis Leadership Approach

1. Recognise the Issue Quickly: Do not delay acknowledging concerns.
2. Investigate Transparently: Gather facts and consult with data protection officers.
3. Take Decisive Action: Suspend or end the partnership if trust is compromised.
4. Communicate Clearly: Inform parents, staff, and students about what happened, what is being done, and how they are protected.
5. Review Policy: Update contract vetting procedures to prevent repeat issues.



Case Study 1: The Free App with Hidden Costs

A school adopted a free "study aid" app promoted as supporting homework. Months later, parents noticed children were receiving targeted ads based on app usage. Investigation revealed that the app was selling student behavioural data.

Leadership Response:

- The contract was terminated immediately.
- Parents were informed with a clear explanation.
- Training was introduced on recognising hidden costs in "free" digital tools.

Lesson: Free digital products often monetise data. Leaders must ensure transparency before adoption.

Case Study 2: The Pressure of Sponsorship

A local business offered a substantial donation to a school in exchange for naming rights to a student award. The award, however, was linked to a product line marketed directly to children.

Leadership Response:

- The headteacher declined the offer, explaining the conflict of interest.
- The refusal was communicated publicly to reinforce ethical standards.
- The school sought alternative community funding sources.

Lesson: Not all money is good money. Ethical alignment must guide partnership decisions.

School's alliances

Building Alliances with Parents and Communities

Partnerships are not only with companies – parents and communities are crucial allies in promoting digital literacy and resilience.

Strategies for Leaders

- Parent Workshops: Offer training on disinformation, cyber safety, and responsible technology use.
- Community Forums: Create open spaces where parents and students can raise concerns about school technology use.
- Shared Responsibility: Encourage families to reinforce the same digital literacy lessons at home.

When parents are involved, trust grows, and students receive consistent guidance across school and home.

Building Alliances with Teachers and Staff

Teachers are frontline implementers of digital initiatives. If they feel excluded from decision-making, partnerships may fail.

Leadership Actions

- Involve teachers in evaluating new tools and contracts.
- Provide time and training for staff to adapt.
- Listen to teacher feedback on student experience with digital platforms.

By treating teachers as co-creators, leaders ensure alliances meet classroom realities, not just administrative goals.

Building Alliances with Students

Students are not passive consumers of technology. They can be active partners in shaping digital environments.

Practical Ideas

- Student Digital Councils: Engage students in reviewing digital tools and policies.
- Peer-Led Workshops: Train older students to mentor younger peers on online safety.
- Feedback Loops: Regularly survey students on their digital learning experiences.

These alliances empower students and build digital citizenship.

Creating a Framework for Ethical Alliances

To systematise decisions, leaders can adopt a simple Ethical Partnership Framework:

1. Purpose: Does this alliance clearly support educational goals?
2. Protection: Are student and staff rights safeguarded?
3. Transparency: Are terms and data uses communicated openly?
4. Equity: Will all students benefit fairly from this partnership?
5. Exit Strategy: Can the school safely withdraw if needed?

Practical Tools for Leaders

Alliance Evaluation Checklist

- Does the contract specify clear data ownership? ☐
- Are parents informed about new digital partnerships? ☐
- Is there an exit strategy without penalties? ☐
- Does the partnership align with school values and child safeguarding standards? ☐
- Are teachers and students involved in the evaluation process? ☐
- Has the agreement been reviewed by legal or safeguarding experts? ☐

Recommended Resources

- Council of Europe Guidelines for Equitable Partnerships between Schools and Companies.[20]
- European Data Protection Board Guidance – data protection in schools.[21]
- UNICEF Guidelines on Digital Partnerships – ethical frameworks for working with tech providers.[22]
- EdTech Evidence Exchange – independent reviews of educational technologies.[23]
- SAILS Project Tools – alliance and contract evaluation checklists.[24]

20 https://rm.coe.int/prems-049222-gbr-2508-ligne-directrice-etablissements-a4-web-1-/1680a94c1b

21 https://www.edpb.europa.eu/our-work-tools/our-documents/topic/children_en

22 https://www.unicef.org/esa/media/3141/file/PolicyLab-Guide-DigitalConnectivity-Nov.6.18-lowres.pdf

23 https://www.nctm.org/research/EdTech/

24 https://sails.deusto.es/

Conclusion

Alliances can empower schools – but they can also compromise them. Leaders must act as vigilant guardians of student safety and institutional integrity.

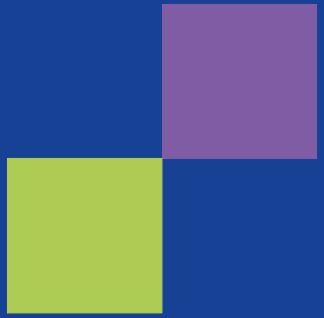
By:

- Evaluating partnerships with critical eyes.
- Promoting ethical digital relationships.
- Responding transparently when problems arise.
- Building strong alliances with teachers, students, parents, and communities.

School leaders can ensure that every alliance strengthens rather than weakens the mission of education.

Ethical, transparent, and equitable partnerships build not only digital literacy but also the trust and resilience of the entire school community.

POLICY DRAFTS FOR SCHOOL LEADERS



1. Model Cyberbullying Policy

Purpose

This policy sets out the school's commitment to preventing, identifying, and addressing bullying and cyberbullying, ensuring a safe and respectful environment for all students and staff.

Scope

This policy applies to:

- Students, staff, and parents engaged in school-related digital interactions.
- Online platforms used for teaching, homework, extracurricular activities, and informal communications that affect the school community.

Definitions

- Bullying: Repeated aggressive behaviour intended to harm or intimidate.
- Cyberbullying: Bullying conducted through digital means such as social media, messaging apps, or online games.

Responsibilities

- School leaders: establish policies, provide resources, and oversee implementation.
- Teachers: monitor student interactions, model respectful behaviour, and intervene when needed.
- Students: report incidents and respect digital conduct guidelines.
- Parents: support school efforts and reinforce respectful behaviour at home.

Procedures

1. Prevention:

- Digital citizenship education included in the curriculum.
- Awareness campaigns run annually for students and parents.

2. Reporting:

- Multiple channels available: anonymous forms, trusted staff, digital reporting tools.

3. Response:

- Incidents documented and investigated promptly.
- Restorative practices prioritised, but disciplinary action taken when necessary.

4. Support:

- Victims receive counselling and staff support.
- Perpetrators offered guidance to change behaviour.

Review

This policy will be reviewed every two years, with input from staff, parents, and students. **HEADstart #25** highlights the importance of coherent organisational policy, which also applies to digital-related documents. A joint review of all digital, safeguarding, and partnership policies; together with the data protection officer and staff representatives –helps ensure that terminology, ethical principles, and legal references are consistent across the whole school.

2. Digital Literacy Framework Outline

Purpose

To ensure that all students and staff develop strong digital literacy skills, enabling them to critically evaluate, use, and create digital content responsibly.

Core Competencies

1. Information Literacy: ability to find, evaluate, and use reliable sources.
2. Critical Thinking: questioning digital content and recognising bias.
3. Digital Resilience: coping with challenges such as cyberbullying or exposure to harmful content.
4. Cybersecurity Awareness: protecting personal and school data.
5. Ethical Use: respecting intellectual property, privacy, and digital rights.

Implementation

- Curriculum integration: digital literacy included across subjects.
- Professional development: ongoing training for teachers.
- Whole-school culture: posters, assemblies, and shared practices promoting critical engagement.

Assessment

- Student portfolios documenting digital projects.
- Teacher reflections and peer reviews.
- Annual review of digital literacy outcomes by school leadership.

3. School Cybersecurity Protocol

Purpose

To protect the digital infrastructure of the school and safeguard sensitive data belonging to students, staff, and parents.

Key Practices

- Passwords: strong, unique passwords required; updated annually.
- Authentication: two-factor authentication for staff accounts.
- Software updates: regular updates and patching of all school systems.
- Backups: secure and regular backups of essential data.
- Device management: clear rules for school-owned and bring-your-own devices.

Roles and Responsibilities

- School leadership: ensure adequate budget and training for cybersecurity.
- IT staff: maintain secure systems, conduct regular audits, and respond to incidents.
- Teachers and staff: follow security protocols, report suspicious activity.
- Students: use devices responsibly and follow security guidelines.

Incident Response

1. Detect and report: any suspected breach must be reported immediately.
2. Contain: isolate affected systems.
3. Investigate: IT staff assess scale and source of breach.
4. Communicate: parents and staff informed promptly with transparent updates.
5. Recover: restore systems and data from secure backups.
6. Review: identify lessons learned and update the protocol.

4. Disinformation Response Protocol

Purpose

To establish a clear process for responding to disinformation or misinformation affecting the school community.

Triggers

- False information circulating about staff, students, or school policies.Rumours on social media affecting trust or safety.

Steps

1. Monitor: designate staff to track emerging issues.
2. Verify: confirm facts quickly with reliable sources.
3. Communicate: share timely, accurate updates with staff, parents, and students via official channels.
4. Educate: use the incident as a teaching opportunity to reinforce media literacy.
5. Escalate: involve local authorities or media if disinformation causes significant harm

5. Alliance and Partnership Policy

Purpose

To ensure school partnerships with technology providers, platforms, and external companies protect student welfare and align with ethical standards.

Principles

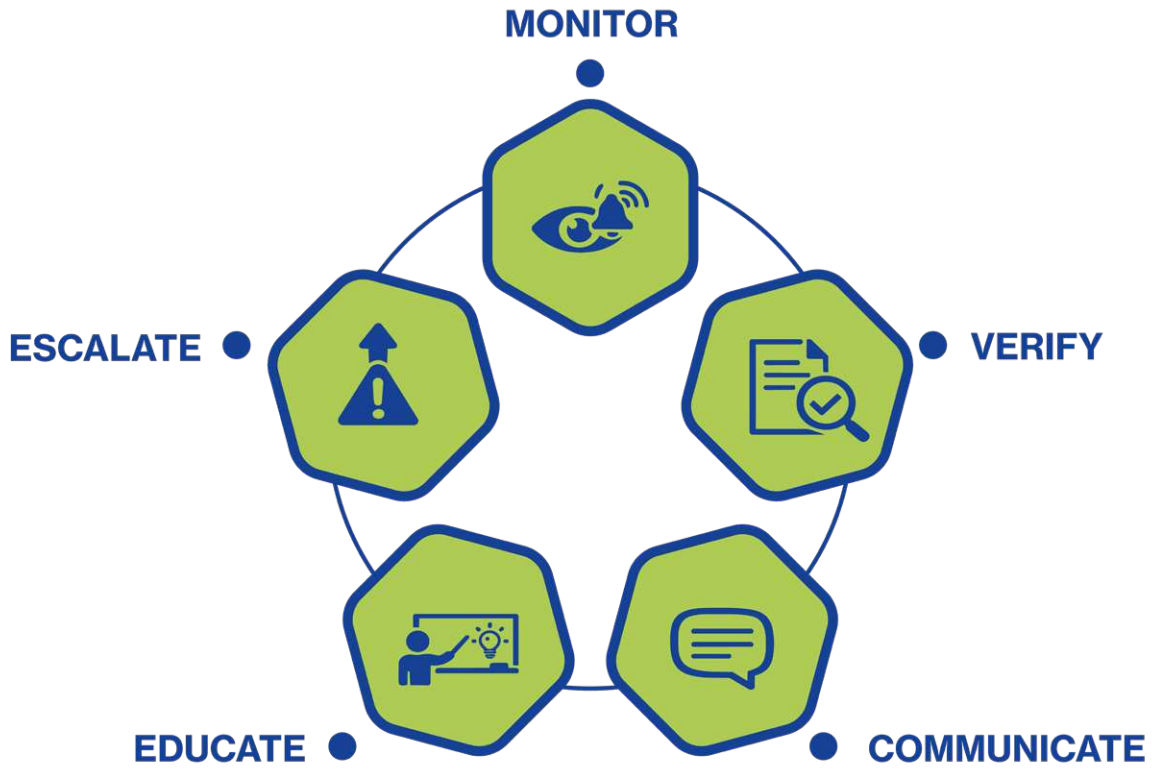
- Transparency: contracts and partnerships explained clearly to parents and staff.
- Privacy: no unnecessary data collection or use of student information.
- Accountability: partners must comply with national and international child protection standards.

Procedures

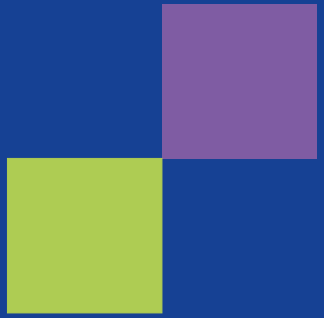
- Review all contracts with IT/legal advisors.
- Involve parents and staff in discussions about new platforms.
- Audit partnerships annually for compliance with privacy and ethics standards.

Case example: A school evaluates a new e-learning platform. Before adoption, the leadership team checks the data collection practices, informs parents, and ensures compliance with GDPR.

DISINFORMATION RESPONSE PROTOCOL



TOOLBOX GUIDES



Professional Competence Development

Start with yourself

Digital literacy and resilience are not just subjects to be taught – they are professional competences. Research from DRONE and related projects shows that professionals who have not developed their own skills often:

- Struggle to model best practices for students.
- Feel overwhelmed by new challenges (e.g., disinformation trends, cybersecurity risks).
- Lack the confidence to lead meaningful school-wide change.

Key principle: You cannot effectively teach what you have not yet mastered yourself.

Step 1: Assess your own digital literacy

Before implementing programmes for students, professionals should measure their starting point. This helps identify strengths and areas for growth.

Example Self-Assessment Test (Teachers/Leaders)

Rate yourself from 1 (not confident) to 5 (very confident).

1. I can recognise when online information is biased or incomplete.
2. I can use at least two different fact-checking methods (e.g., reverse image search, fact-checking sites).
3. I know the difference between misinformation, disinformation, and satire.
4. I can explain privacy settings and cybersecurity basics to colleagues or students.
5. I feel confident responding to a parent or student who shares false or misleading information.
6. I can manage my own digital wellbeing (e.g., balance, coping with negativity online).
7. I understand how contracts with digital platforms may affect student data.

Scoring:

- 30–35 = High competence. Ready to model and lead.
- 20–29 = Moderate competence. Identify areas for targeted training.
- Below 20 = Significant support needed before teaching others.

Step 2: Professional Development Pathways

- Short courses: Engage with asynchronous modules (e.g., DRONE's online course, UNESCO Media Literacy curriculum).
- Peer learning: Set up professional learning communities where teachers practice fact-checking or share resilience strategies.
- External training: Attend workshops from trusted organisations (OECD, European Schoolnet, Common Sense Education).
- Reflection logs: Keep a digital journal of challenges faced and strategies learned.

Step 3: Ongoing Reflection and Modelling

- Be transparent with students about your own learning process.
- Share personal experiences of mistakes online – this normalises critical reflection.
- Regularly update your skills as platforms, tools, and risks evolve.

Case study: "Leading by learning first"

A school leader realised that staff were not confident teaching about fake news. Before launching a student program, she arranged a two-day staff training where teachers practiced identifying disinformation, took self-tests, and reflected on personal online habits. Only after this did the school introduce a student-focused initiative. Staff reported feeling more empowered and authentic as role models.

Step 4: Map Your Info Flow

Draw a daily timeline, and include all sources of digital information you interacted with (e.g., WhatsApp, news sites, school emails, Instagram, etc.)

Reflection questions:

- What patterns do you see?
- What sources do you trust most?
- What sources do you trust least?

Addressing Bullying by Teachers

Why this matters

While much focus is rightly placed on peer-to-peer bullying, DRONE research and international studies reveal a critical gap: students can also experience bullying from teachers or other school staff. This may involve:

- Humiliation in front of peers.
- Unfair or repeated targeting.
- Abuse of power in grading, discipline, or classroom dynamics.
- Online harassment or inappropriate digital communication.

Such experiences are deeply damaging. They undermine trust in education, harm wellbeing, and set a poor example for students.

Preventive Measures for School Leaders

- Zero tolerance policy: Make clear that bullying by staff is unacceptable and carries consequences.
- Code of conduct: Include respectful digital and in-person behaviour in staff policies.
- Confidential reporting systems: Ensure students (and parents) can report teacher bullying safely.
- Regular training: Include modules on power dynamics, empathy, and appropriate digital communication.
- Observation and accountability: Use peer observations, student surveys, and leadership walkthroughs to detect early warning signs.

Preventive Measures for Teachers

- Reflective practice: Regularly ask, “Could my words or actions be perceived as humiliating or targeting a student?”
- Language awareness: Avoid sarcasm, public shaming, or comparisons that single out students negatively.
- Discipline with dignity: Apply rules consistently, explain reasoning, and avoid personal attacks.
- Digital boundaries: Keep all online communication with students professional, transparent, and school-approved.

When Things Go Wrong

If a teacher is accused of bullying a student:

- Immediate response: Take the allegation seriously; ensure the student feels safe.
- Investigation: School leadership must investigate promptly, fairly, and confidentially.
- Support: Provide emotional support to the student. Offer professional development or disciplinary measures for the teacher, depending on severity.
- Restorative practices: Where possible, use restorative dialogue to rebuild trust.

Case study 1: "The sarcastic teacher"

A secondary school teacher frequently mocked students for wrong answers. One student began skipping lessons, claiming illness. Parents reported the issue. The school leader conducted confidential interviews, confirming the pattern. The teacher was required to attend training on classroom communication and was mentored by a senior colleague. A restorative meeting was held with the affected student. The student returned to class, and the teacher reported greater awareness of language use.

Case study 2: "Crossing digital lines"

A teacher used a private messaging app to contact students about homework, sometimes sending late-night critical messages. Students felt pressured and humiliated. The school investigated and established a new policy: all digital communication must go through the official school platform. Training was provided on digital boundaries.

Key Takeaways for Teachers and Leaders

1. Develop yourself first – Digital literacy begins with self-reflection and competence-building.
2. Measure and improve – Use self-tests to identify growth areas.
3. Model good practice – Students and staff learn most from what you do, not just what you say.
4. Address all forms of bullying – Including the often-hidden issue of teacher-to-student bullying.
5. Create safe systems – Reporting, investigation, and support must be transparent and trusted.

Personal development checklists

Part 1: Digital Literacy Skills Self-Test for Professionals

Instructions

This self-test helps you identify your digital literacy strengths and areas for growth before teaching or implementing student programmes.

- Rate yourself 1 (not confident at all) to 5 (very confident).
- Be honest – this is for self-reflection, not evaluation by others.

Section A: Information Literacy

1. I can evaluate the credibility of an online article or video. ☐
2. I can identify the purpose and bias behind a source. ☐
3. I use fact-checking tools (e.g., reverse image search, Snopes, Full Fact). ☐
4. I can teach others to compare multiple sources effectively. ☐

Score A: ___ / 20

Section B: Disinformation Awareness

5. I can explain the difference between misinformation, disinformation, and satire. ☐
6. I recognise common red flags of fake news. ☐
7. I can respond constructively when someone shares misinformation. ☐
8. I stay informed about current disinformation trends. ☐

Score B: ___ / 20

Section C: Resilience & Problem-Solving

9. I know strategies to cope with negativity or harassment online. ☐
10. I feel confident modelling resilience to colleagues and students. ☐
11. I can guide students through digital dilemmas using structured problem-solving. ☐
12. I maintain a healthy balance between my online and offline life. ☐

Score C: ___ / 20

Section D: Critical Thinking

13. I routinely question evidence and identify bias in digital content. ☐
14. I integrate critical thinking practices into my teaching. ☐
15. I can support students in evaluating conflicting information. ☐
16. I can spot when conspiracy or extremist content influences classroom discussions. ☐

Score D: ___ / 20

Section E: Cybersecurity

17. I use strong, unique passwords and two-factor authentication. ☐
18. I keep devices and software updated. ☐
19. I recognise signs of phishing attempts or scams. ☐
20. I know how to protect student data in the classroom. ☐

Score E: ___ / 20

Scoring Guide

80–100: High competence. Ready to model and lead.

60–79: Moderate competence. Identify growth areas.

40–59: Basic competence. Significant professional development recommended.

Below 40: Urgent need for structured training before teaching these skills to students.

Reflection Prompts

- Which areas did I score lowest in?
- How could I improve those skills in the next 6 months?
- What training, peer support, or resources would help me most?

Part 2: Bullying Prevention Checklist for Staff

Purpose

To prevent bullying in all forms, including the often-overlooked issue of teacher-to-student bullying.

For Teachers (Self-Check)

- I use respectful language even when correcting mistakes. ☐

- I avoid sarcasm, ridicule, or public humiliation. ☐
- I apply discipline consistently and fairly. ☐
- I reflect regularly: could my actions be perceived as targeting a student? ☐
- I keep all digital communication with students professional and transparent. ☐
- I seek feedback from colleagues or mentors on my classroom tone. ☐
- I know how to respond if I witness a colleague bullying a student. ☐

For School Leaders (Monitoring & Support)

- A clear code of conduct exists that includes teacher-to-student interactions. ☐
- Confidential reporting systems are in place for students and parents. ☐
- Staff receive regular training on empathy, communication, and power dynamics. ☐
- Classroom observations or student surveys monitor staff-student relationships. ☐
- Reports of bullying by teachers are investigated promptly and fairly. ☐
- Support (counselling, mentoring, or training) is provided to both victims and staff involved. ☐
- Disciplinary procedures are clear and enforced when necessary. ☐

Case Reflection Tool (for staff meetings)

- Describe a situation where a student felt targeted by a teacher.
- How could it have been handled differently?
- What safeguards could prevent this happening again?

Professional Development Roadmap For Teachers and School Leaders

Phase 1: Baseline and Awareness (Months 1–2)

Goals

- Establish a clear understanding of current competence levels.
- Raise awareness of digital literacy, disinformation, and bullying risks.

Actions

- Administer the Digital Literacy Skills Self-Test to all staff.
- Collect anonymous results to identify whole-school strengths and gaps.
- Hold an introductory workshop: "Why Digital Literacy and Resilience Matter for Schools."
- Share case studies from the DRONE handbooks to illustrate real challenges.

Outputs

- Baseline report of staff competence.
- Awareness raised among staff and leadership.

Phase 2: Personal Skill Development (Months 3–5)

Goals

- Strengthen individual competences before teaching students.
- Encourage reflection and personal responsibility.

Actions

- Offer short online courses (e.g., DRONE asynchronous modules, UNESCO MIL course https://www.unesco.org/en/media-information-literacy/moocs).
- Organise peer-learning groups: teachers practice fact-checking, identify fake news, and reflect on digital resilience.
- Provide access to recommended reading lists and toolkits.
- Encourage each teacher to set one personal digital skill goal (e.g., mastering reverse image search, improving password security).

Outputs

- Staff increase personal confidence in digital literacy.
- Peer-support networks established.

Phase 3: Classroom Integration Pilots (Months 6–8)

Goals

- Begin experimenting with integrating digital literacy into teaching.
- Focus on modelling skills, not yet full programmes.

Actions

- Teachers pilot 1–2 classroom activities from the Lesson Plan Toolkit (e.g., spotting fake news exercise).
- School leaders host reflection sessions to share successes and challenges.
- Introduce the Bullying Prevention Checklist with emphasis on teacher-to-student behaviour.
- Collect student feedback on pilot lessons: What worked? What confused them?

Outputs

- Early evidence of what integration looks like in practice.
- Staff self-awareness around language and behaviour with students.

Phase 4: Whole-School Implementation (Months 9–10)

Goals

- Scale digital literacy into school culture and curriculum.
- Establish policies and systems to support long-term work.

Actions

- Finalise and adopt a Digital Literacy Framework for the school.
- Launch school-wide awareness campaigns (assemblies, posters, newsletters for parents).
- Implement anti-bullying policies that explicitly include staff-student dynamics.
- Deliver resilience workshops for both staff and students.

Outputs

- Digital literacy embedded across multiple subjects.
- Whole-school anti-bullying policy in place.
- Shared culture of resilience and critical engagement.

Phase 5: Review and Consolidation (Months 11–12)

Goals

- Measure progress and refine practices.
- Ensure sustainability of professional development.

Actions

- Re-administer the Digital Literacy Skills Self-Test to all staff.
- Compare results with baseline to track growth.
- Collect case studies of classroom and school initiatives that worked.
- Update the professional development plan for the following year.

Outputs

- Evaluation report showing skill growth.
- Refined roadmap for Year 2 (deeper focus on cybersecurity, alliances with companies, parent partnerships).

Ongoing Supports Throughout the Year

- Peer coaching: monthly small-group meetings where teachers support each other.
- Leadership check-ins: quarterly staff surveys to monitor digital culture.
- Student voice: feedback mechanisms so students can reflect on digital literacy lessons and teacher conduct.
- Parent engagement: workshops and newsletters to align home and school approaches.

Case Example: A One-Year Transformation

At the start of the year, a secondary school found that 65% of staff scored below “moderate competence” in the self-test. Students were reporting misinformation in class and occasional incidents of teacher sarcasm escalating to bullying complaints.

By the end of the roadmap:

- Staff re-tests showed a 25% average increase in confidence across all domains.
- A new digital literacy framework was integrated into English, science, and social studies.
- Student feedback noted they felt safer discussing online challenges in class.
- A clear anti-bullying code for both staff and students was adopted.

School Leader Quick Reference Guide

(A companion to the DRONE School Leader Handbook)

1. Digital Literacy & Disinformation: Leadership Priorities

Your Role as a Leader

- Set a whole-school culture of critical thinking and safety.
- Model responsible digital behaviour in your own communication.
- Provide clear frameworks, policies, and training for staff.
- Engage parents and students in open conversations about digital challenges.

Red Flags

- Staff unsure how to respond to fake news or digital rumours.
- Parents distrusting school communications due to misinformation.
- Students repeating unverified or extreme claims without questioning.

2. Information Literacy

Leadership Actions

- Embed source-checking and evaluation skills across the curriculum.
- Support teachers with classroom-ready fact-checking strategies.
- Provide staff training in handling misinformation.

Red Flags

- Teachers relying on a single online source for classroom material.
- Students struggling to distinguish fact from opinion.
- Disputes in school triggered by rumours or unchecked claims.

3. Resilience Building

Leadership Actions

- Train staff to spot early signs of digital distress.
- Provide counselling and peer support systems for students.
- Promote digital wellbeing (screen breaks, healthy boundaries).

Red Flags

- Staff showing burnout from digital overload.
- Students avoiding devices due to anxiety.
- Escalating online conflicts spilling into school life.

4. Problem-Solving in a Digital World

Leadership Actions

- Encourage creative solutions to digital dilemmas.
- Provide professional development for staff in online conflict resolution.
- Include students in shaping school digital policies.

Red Flags

- Teachers escalating digital conflicts rather than de-escalating.
- Students disengaging when digital issues arise.
- Lack of clarity about “what to do” in online problem scenarios.

5. Critical Thinking

Leadership Actions

- Promote questioning culture: “Who wrote this? Why? What’s missing?”
- Integrate critical thinking across all subjects, not just ICT.
- Support teachers with toolkits and resources for classroom use.

Red Flags

- Students (or staff) believing and spreading conspiracy-style claims.

- Classroom discussions shut down instead of explored critically.
- Staff uncomfortable modelling critical questioning.

6. Bullying & Cyberbullying

Leadership Actions

- Establish zero-tolerance policies for all bullying – by teachers, family members, or peers.
- Create confidential reporting channels for students and parents.
- Train staff to handle digital evidence (screenshots, messages).
- Use restorative approaches where safe, but act firmly where harm is serious.

Red Flags

- Reports of teacher–student humiliation dismissed as “discipline.”
- Family bullying overlooked because it happens “at home.”
- Viral videos or online harassment causing reputational damage.

7. Cybersecurity

Leadership Actions

- Require annual staff training (phishing awareness, password hygiene).
- Ensure offline backups of critical systems.
- Have a tested incident response plan for breaches.
- Teach students age-appropriate cybersecurity practices.
- Involve parents in home cybersecurity awareness.

Red Flags

- Staff using the same password for multiple systems.
- Unsecured personal devices connected to school networks.
- No clear procedure for reporting suspicious emails.

8. Building Alliances

Leadership Actions

- Scrutinise every contract: data ownership, transparency, exit strategy.

- Prioritise ethical partnerships that safeguard students.
- Engage teachers, parents, and students in evaluating digital tools.
- Build alliances with community organisations, universities, and NGOs.

Red Flags

- "Free" apps monetising student data.
- Sponsors pressuring the school to promote products.
- Parents discovering hidden data-sharing without their knowledge.

Crisis Response Checklist

When a digital incident escalates (rumour, data breach, cyberbullying):

1. Contain – stop the immediate harm. ☐
2. Verify – gather facts before speaking. ☐
3. Communicate – inform staff, parents, and students with clarity. ☐
4. Support – provide counselling or safeguarding help to those affected. ☐
5. Review – update policies and training to prevent recurrence. ☐

Top 10 Leadership Habits for a Digitally Safe School

1. Use strong, unique passwords (or a password manager).
2. Keep your own devices secure and updated.
3. re clear digital safety expectations with staff and students.
4. Review all external contracts with legal and safeguarding advisors.
5. Schedule annual staff training on digital literacy and cybersecurity.
6. Involve parents and students in shaping policies.
7. Promote open reporting channels for bullying or online issues.
8. Model transparency and responsible communication.
9. Back up data regularly and test recovery systems.
10. Celebrate digital resilience and critical thinking successes.

ANNEXES

Annex 1

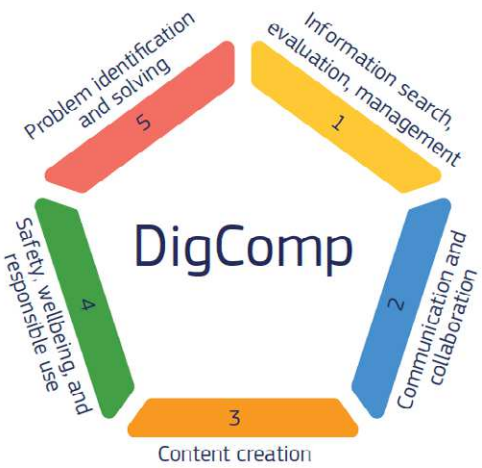
5 Areas of the Digital Competence Framework for Citizens (DigComp)

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.

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 modeling 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!

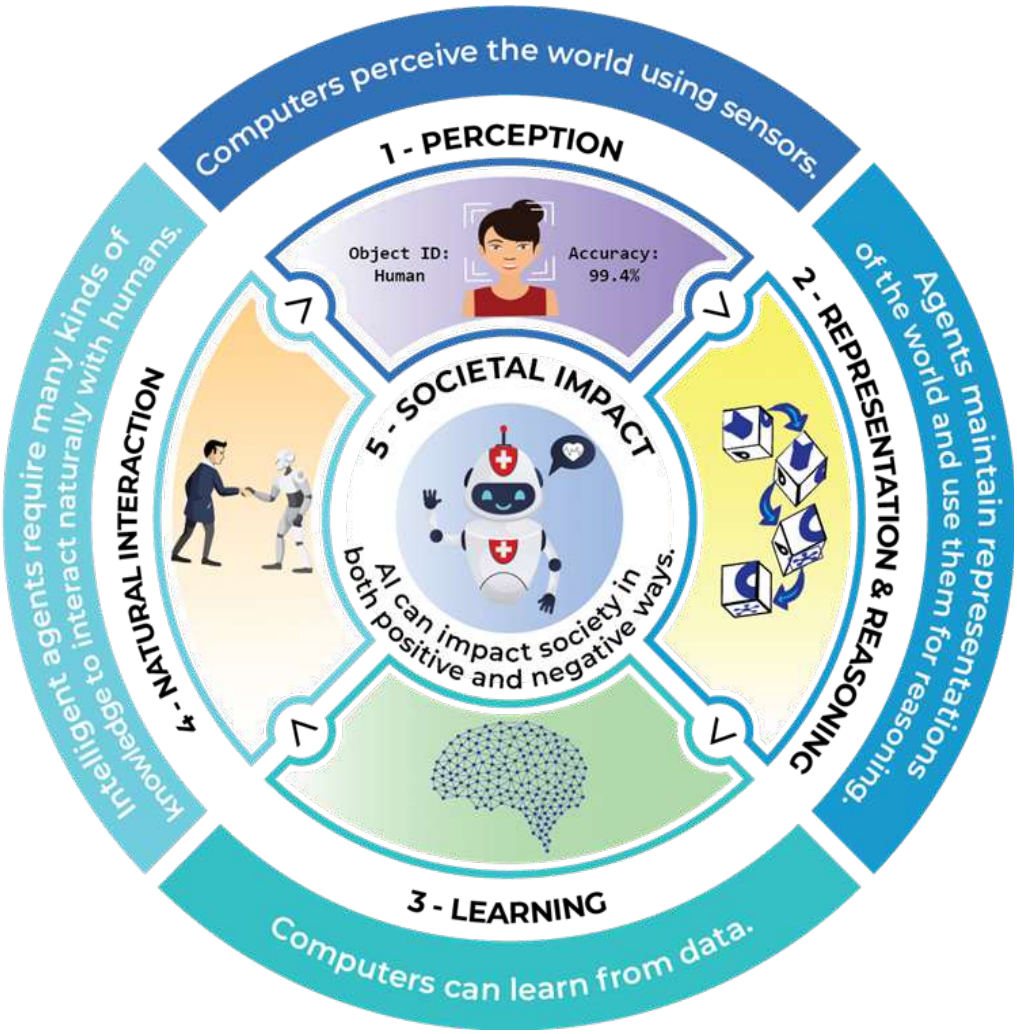
Empowering, not enabling

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:

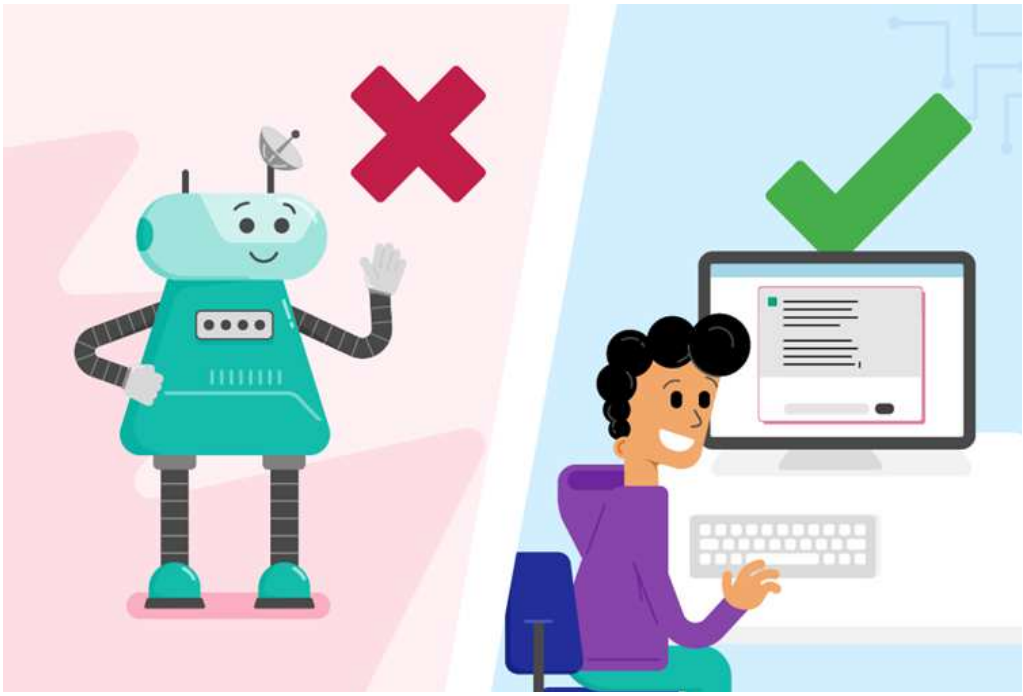
- Perception: compare the way an AI system “perceives” the world with the way humans do
- Representation and reasoning: the representations of the world AI developers can use to create models
- Learning: how the model is trained, the accuracy required and how the training data is checked for bias
- Natural 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.

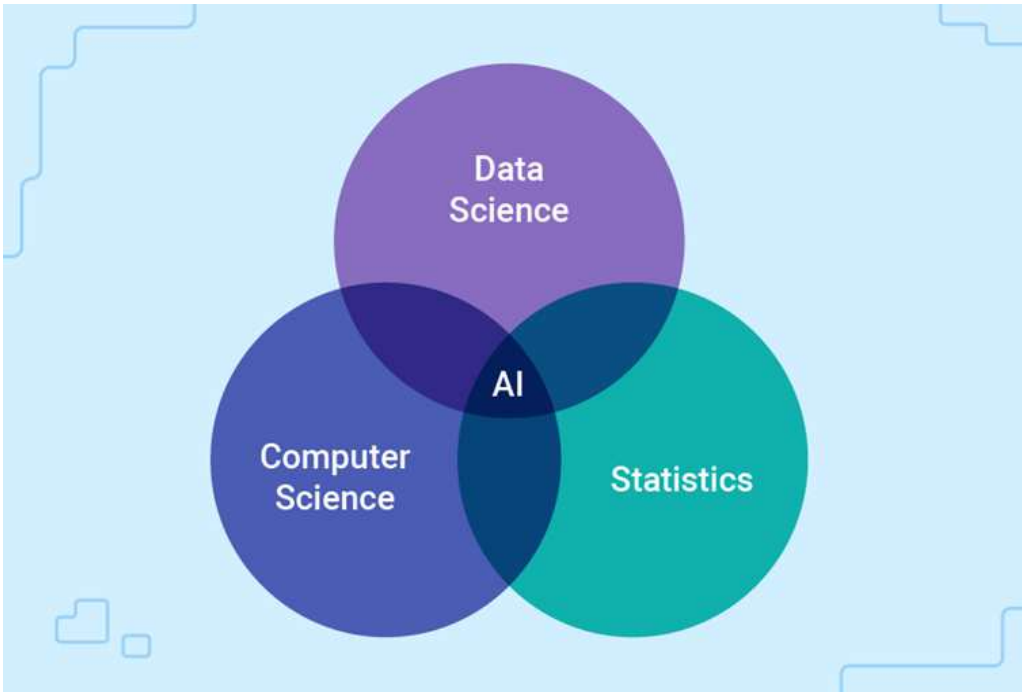
AI is an area of research that includes the use of computer science, data science, and statistics to solve the problems facing us today. Researchers from all these areas and many more are interested to see how computers can help us solve increasingly complex problems by using the large amounts of data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

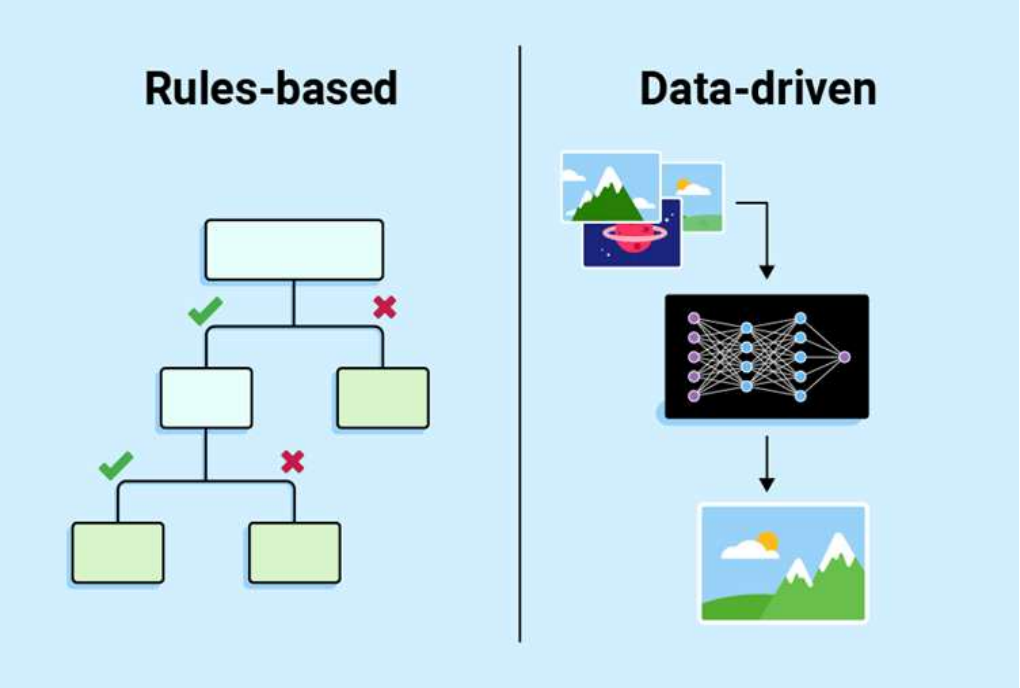
Rules-based systems

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.

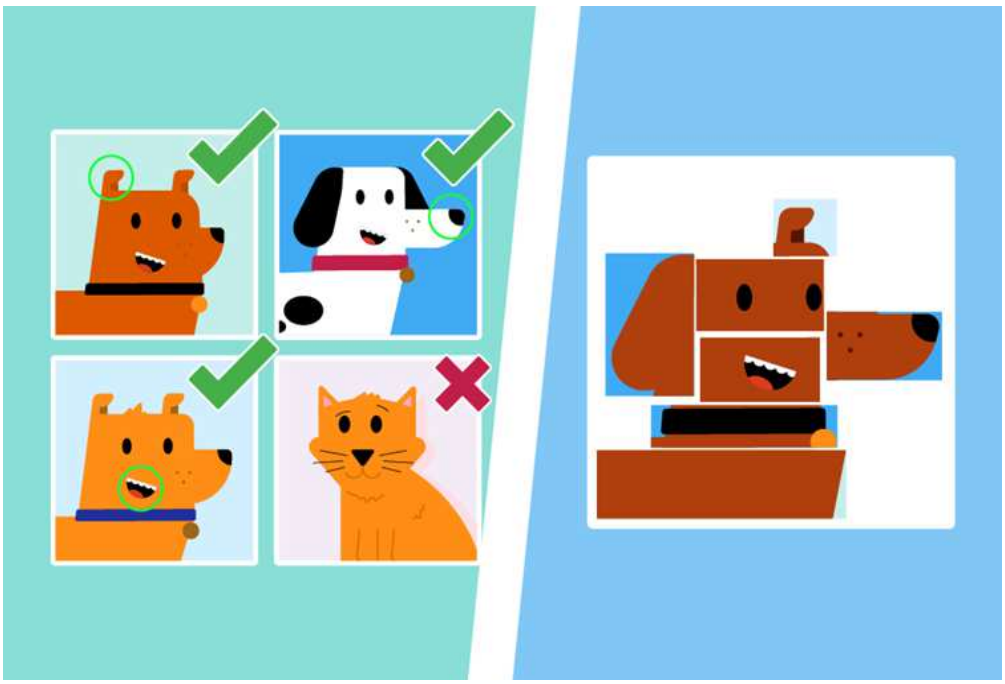
In general terms, bias refers to a prejudice in favour of or against one thing, person, or group compared with another, usually in a way considered to be unfair.

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 Ecgbert 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 – 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.

The DRONE Consortium

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

Associated Partner

	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