ESPLORATORE DIGITALE

Manuale DRONE per Dirigenti Scolastici

Funded by
the European Union

Questo manuale è stato redatto nel 2025 nell'ambito del progetto DRONE finanziato dall'UE. È stato revisionato e preparato per la pubblicazione digitale nel 2026. Per la prima versione delle traduzioni è stato utilizzato DeepL Translator Pro; nessun altro strumento di intelligenza artificiale è stato utilizzato nella creazione dei contenuti del manuale e degli altri manuali di questa serie di tre volumi.

Il libro è stato progettato e impaginato per la distribuzione in formato PDF utilizzando Adobe Creative Cloud, con particolare attenzione alla leggibilità sullo schermo e alla lettura digitale di testi lunghi.

Prima edizione digitale (PDF) pubblicata nel 2026.

© 2026 Eszter Salamon, Aristidis Protopsaltis

Editor: Judit Horgas

Design: Emanuele Bertolani



CC BY-NC-SA 4.0

Creative Commons Attribution: Non commerciale - Condividi allo stesso modo 4.0 Internazionale. Questa licenza richiede che i riutilizzatori attribuiscano il merito al creatore. Consente ai riutilizzatori di distribuire, remixare, adattare e sviluppare il materiale in qualsiasi mezzo o formato, solo per scopi non commerciali.

- BY: Il credito deve essere attribuito a te, il creatore.
- NC: È consentito solo l'uso non commerciale della tua opera.
- SA: Se remixate, trasformate o sviluppate il materiale, dovete distribuire i vostri contributi con la stessa licenza dell'originale.

Per uso non commerciale si intende un uso non destinato principalmente o finalizzato al conseguimento di un vantaggio commerciale o di un compenso monetario.

È possibile condividere e adattare questo materiale per scopi non commerciali, purché venga citata la fonte, vengano indicate le modifiche apportate e qualsiasi opera derivata sia distribuita con la stessa licenza.

Una copia della licenza è disponibile all'indirizzo:

https://creativecommons.org/licenses/di-nc-sa/4.0/

ISBN: [ISBN, if applicable]

Formato file: PDF

Pubblicato da Parents International, membro del consorzio DRONE Project

I manuali DRONE sono pensati per essere utilizzati da genitori o tutori, insegnanti, dirigenti scolastici e formatori. Il loro scopo principale è quello di promuovere l'alfabetizzazione digitale e contrastare la disinformazione. I manuali sono flessibili e possono essere adattati a vari contesti e alle esigenze individuali. Per alcuni utenti, costituiscono un'introduzione accessibile ai fondamenti dell'alfabetizzazione digitale e della disinformazione, presentando concetti e pratiche essenziali in un linguaggio semplice. Per altri, i manuali offrono una guida pratica su come integrare i temi dell'alfabetizzazione digitale e della disinformazione nelle attività didattiche rivolte ai giovani, sia in contesti scolastici formali che in ambienti educativi non formali. Inoltre, i manuali sono risorse preziose per chi progetta programmi o corsi di alfabetizzazione digitale e disinformazione per altri educatori o formatori. Nelle scuole e in contesti educativi formali simili, si raccomanda di coordinarsi con i responsabili della protezione dei dati dell'istituzione quando si utilizzano questi manuali.

INDICE

Capitolo 1 - Alfabetizzazione dell'informazione.....17

Capitolo 2 - Disinformazione, misinformazione e fake news.....27

Capitolo 3 - Sviluppo della resilienza.....35

Capitolo 4 - Risoluzione dei problemi.....45

Capitolo 5 - Pensiero critico.....55

Capitolo 6 - Bullismo e cyberbullismo….....67

Capitolo 7 - Cybersecurity.....79

Capitolo 8 - Costruire alleanze.....89

Modelli di linee guida per dirigenti scolastici.....99

Strumenti.....107

Allegati.....127

Questo manuale è stato concepito come guida strategica e operativa per orientare la cultura digitale della vostra scuola. Supporta i dirigenti scolastici nella definizione della cultura digitale dell'intero istituto, nelle pratiche di salvaguardia, nello sviluppo del personale e nelle risposte alla disinformazione e ai rischi digitali.

L'alfabetizzazione digitale nelle scuole non è più facoltativa, ma piuttosto un elemento fondamentale della leadership scolastica: influisce sul benessere, sulla fiducia, sulla qualità dell'insegnamento e sulla reputazione pubblica della scuola. Questo manuale aiuta i dirigenti ad affrontare queste sfide in modo proattivo e responsabile.

Come trarre da questo manuale il massimo vantaggio

Iniziate con una visione panoramica complessiva: utilizzate l'introduzione e i primi capitoli per comprendere le implicazioni più ampie dell'alfabetizzazione digitale per la cultura organizzativa della scuola, per la gestione e per le responsabilità della dirigenza.

1. Valutate i vostri punti di forza e le vostre lacune in materia di leadership. Gli strumenti di riflessione aiutano a identificare le aree di miglioramento:

- Processi di valutazione dei rischi
- Esigenze di formazione del personale
- Sicurezza informatica e preparazione alle minacce informatiche
- Sistemi di comunicazione
- Valutazione degli strumenti e delle piattaforme digitali

Utilizzatelo per identificare le priorità e assegnare le responsabilità.

2. Utilizzate i capitoli come cornici d'azione. Ogni capitolo include passaggi pratici, considerazioni politiche e scenari che potete utilizzare per informare le decisioni della leadership, le valutazioni dei rischi e la pianificazione a livello scolastico.

3. Sostenete lo sviluppo del personale. Utilizzate le strategie incentrate sugli insegnanti per progettare sessioni di sviluppo professionale continuo, programmi di mentoring e iniziative di apprendimento collaborativo.

4. Rafforzate i sistemi scolastici nel loro complesso. Il manuale include linee guida per:

- sviluppare o aggiornare le politiche anti-bullismo
- valutare gli strumenti digitali e le partnership esterne
- definire aspettative chiare per la condotta del personale
- creare dei sistemi di comunicazione resilienti con le famiglie
- prevenire e rispondere alle crisi di disinformazione

5. Imparate dai casi di studio. I casi di studio si basano su situazioni reali affrontate dalle scuole. Possono essere utilizzati per discussioni del gruppo dirigente, formazione del

personale e pianificazione di scenari.

6. Rivedeteli durante le crisi. Quando si verifica un incidente legato a disinformazione, cyberbullismo, uso improprio di strumenti digitali, le sezioni “quando le cose vanno male” forniscono misure immediate per stabilizzare la situazione.

Una risorsa per la leadership

Questo manuale vi aiuta a creare un ambiente digitale sicuro, etico e pronto per il futuro. Utilizzatelo per rafforzare la fiducia del personale, proteggere gli studenti, costruire un rapporto di fiducia con le famiglie e prendere decisioni informate in un panorama digitale in rapida evoluzione.

Se volete approfondire

I moduli di leadership del corso online DRONE forniscono una guida avanzata sulla comunicazione di crisi, la salvaguardia digitale e la pianificazione strategica.

Accedete al sito web DRONE qui: https://mydroneproject.eu/

COME UTILIZZARE QUESTO MANUALE

Le risorse DRONE – una raccolta di moduli formativi e tre manuali – sono state progettate come una serie completa e interconnessa di strumenti a supporto dell'alfabetizzazione digitale, della resilienza, del comportamento responsabile online e della prevenzione dei danni digitali nell'intera comunità scolastica. Ciascuna risorsa svolge un ruolo diverso, ma insieme forniscono un sistema di supporto a 360 gradi che coinvolge studenti, famiglie, insegnanti e gruppi dirigenti. Lo scopo di questa raccolta di risorse è semplice ma potente: costruire una comunità di apprendimento digitalmente sicura, criticamente consapevole ed emotivamente resiliente.

È possibile utilizzare le risorse singolarmente o come sistema integrato, a seconda delle proprie esigenze. Ogni risorsa, dai capitoli completi alle brevi guide, rappresenta un passo avanti verso tale obiettivo.

Cosa è incluso?

1. Tre manuali completi

Ogni manuale è pensato per un pubblico diverso:

- Manuale DRONE per genitori
- Manuale DRONE per insegnanti
- Manuale DRONE per dirigenti scolastici

Sebbene la struttura sia comune, ogni libro include casi di studio, strategie e responsabilità specifici per i lettori di riferimento. Il manuale per genitori si concentra sulle pratiche quotidiane in ambito domestico; il manuale per insegnanti si concentra sulla pedagogia; il manuale per dirigenti scolastici si concentra sulle azioni di carattere normativo e organizzativo.

2. Moduli di formazione per insegnanti, dirigenti scolastici e genitori

Ogni modulo formativo è disponibile in tre diversi formati. È stata sviluppata una versione online per l'apprendimento autonomo e sono disponibili risorse scaricabili per organizzare una sessione di formazione in presenza o online sincrona.

Ciascuno dei tre gruppi target può scegliere tra diversi moduli formativi che possono essere utilizzati indipendentemente dagli altri moduli sui seguenti argomenti:

- Alfabetizzazione informatica
- Disinformazione, misinformazione e fake news
- Sviluppo della resilienza
- Risoluzione dei problemi
- Pensiero critico
- Bullismo e cyberbullismo
- Sicurezza informatica

- Costruire alleanze

Come i pezzi stanno insieme

Genitori

- Iniziate con il Manuale per genitori per una comprensione completa.
- Utilizzate la Guida rapida alla sicurezza informatica, il Kit contro il bullismo e la Guida alla conversazione per un supporto quotidiano.
- Esplorate gli elenchi di letture per sviluppare una consapevolezza digitale a lungo termine a casa.
- Se desiderate approfondire l'argomento e non avete mai seguito una formazione su questo tema, consultate il modulo di formazione pertinente per saperne di più.
- Se ritenete che gli insegnanti debbano approfondire le loro conoscenze, consigliate loro le risorse didattiche.

Insegnanti

- Iniziate con il Manuale per insegnanti per sviluppare le vostre competenze digitali.
- Tenete la Guida di riferimento rapido per insegnanti nella vostra classe o nella sala professori.
- Utilizzate gli strumenti rivolti agli studenti (Guida alla sopravvivenza digitale, ecc.) nelle vostre lezioni.
- Fate riferimento ai casi di studio e ai toolkit durante gli incidenti che coinvolgono disinformazione, bullismo o conflitti online.
- Se desiderate approfondire l'argomento e non avete mai seguito una formazione su un determinato tema, consultate il modulo di formazione pertinente per saperne di più.
- Se ritenete che genitori di studenti della vostra scuola abbiano bisogno di maggior supporto, consigliate loro le risorse per genitori.

Dirigenti Scolastici

- Utilizzate il Manuale per i dirigenti per definire le azioni da intraprendere, le modalità di valutazione dei rischi e l'approccio al digitale che caratterizza la vostra scuola.
- Condividete le guide rapide con personale e genitori per creare una visione comune.
- Utilizzate i toolkit per supportare la formazione del personale e il coinvolgimento della comunità.
- Fate riferimento alle liste di letture, alle sintesi delle ricerche e alle risorse per gli insegnanti quando progettate la formazione continua.
- Se desiderate approfondire un argomento e non avete mai seguito una formazione su di esso, consultate il modulo di formazione pertinente per saperne di più.
- Se ritenete che i genitori di studenti della vostra scuola abbiano bisogno di maggiore supporto, consigliate loro le risorse per genitori.

DOVE TROVARE LE INFORMAZIONI IN QUESTO MANUALE

Trovate il vostro percorso in questo manuale (cliccate per accedere alla sezione desiderata)

CHE COSA MI SERVE ORA?

PERCORSO 1
Sviluppare leadership per quanto riguarda l'alfabetizzazione digitale

- **INTRODUZIONE** Il ruolo dei dirigenti (p.13)
- **CAPITOLO 1** Alfabetizzazione dell'informazione (pp.17-26)
- **CAPITOLO 2** Disinformazione, misinformazione & fake news (pp.27-34)

PERCORSO 2
Sviluppare resilienza e capacità di problem-solving

- **CAPITOLO 3** Sviluppare la resilienza (pp.35-44)
- **CAPITOLO 4** Problem-solving (pp.45-54)

PERCORSO 3
Affrontare rischi e incidenti concreti

- **CAPITOLO 6** Bullismo e Cyberbullismo (pp.67-78)
- **CAPITOLO 7** Cybersecurity (pp.79-88)
- **STRUMENTI** (pp.107-124)

PERCORSO 4
Costruire politiche e alleanze

- **CAPITOLO 5** Pensiero critico (pp.55-64)
- **CAPITOLO 8** Costruire alleanze (pp.89-98)
- **STRUMENTI** (pp.107-124)

INTRODUZIONE: ALFABETIZZAZIONE DIGITALE E DISINFORMAZIONE - IL RUOLO DELLE SCUOLE

Nel mondo odierno, gli ambienti digitali influenzano quasi ogni aspetto della vita dei giovani. Gli studenti imparano, comunicano, giocano e persino costruiscono la propria identità in spazi mediati dalla tecnologia. Questa realtà digitale offre enormi opportunità: accesso alla conoscenza, espressione, creatività e collaborazione globale. Tuttavia, comporta anche gravi rischi. Tra i più urgenti vi sono la diffusione di misinformazione, disinformazione e contenuti nocivi.

Le scuole sono al centro di questa sfida. Non sono solo centri di apprendimento, ma anche spazi fondamentali in cui gli studenti possono sviluppare le abitudini, le competenze e la resilienza necessarie per orientarsi in una società digitale. A differenza degli ambienti online informali, le scuole offrono opportunità strutturate per porre domande, riflettere e confrontarsi in modo critico con le informazioni. Possono fungere da ambienti protettivi in cui le misinformazioni vengono contestate, le fake news smascherate, e i giovani imparano a partecipare in modo responsabile alle comunità digitali.

In questo contesto, i dirigenti svolgono un ruolo fondamentale. Sono loro a stabilire la direzione della scuola, a definire le priorità e a creare la cultura all'interno della quale interagiscono insegnanti e studenti. Quando i dirigenti scolastici considerano l'alfabetizzazione digitale come essenziale, essa viene integrata nel programma scolastico e nella vita della scuola in generale. Al contrario, se la dirigenza trascura queste questioni, si creano delle lacune che possono lasciare gli studenti impreparati, gli insegnanti senza sostegno e le comunità vulnerabili.

Perché l'alfabetizzazione digitale è importante per i dirigenti

L'alfabetizzazione digitale viene spesso fraintesa come una questione puramente tecnica: sapere come utilizzare i dispositivi, accedere alle piattaforme o utilizzare applicazioni specifiche. In realtà, è molto più ampia. L'alfabetizzazione digitale comprende la capacità di cercare, valutare, interpretare e rispondere alle informazioni. Richiede consapevolezza critica ed etica: sapere non solo come utilizzare la tecnologia, ma anche perché, quando e con quali conseguenze.

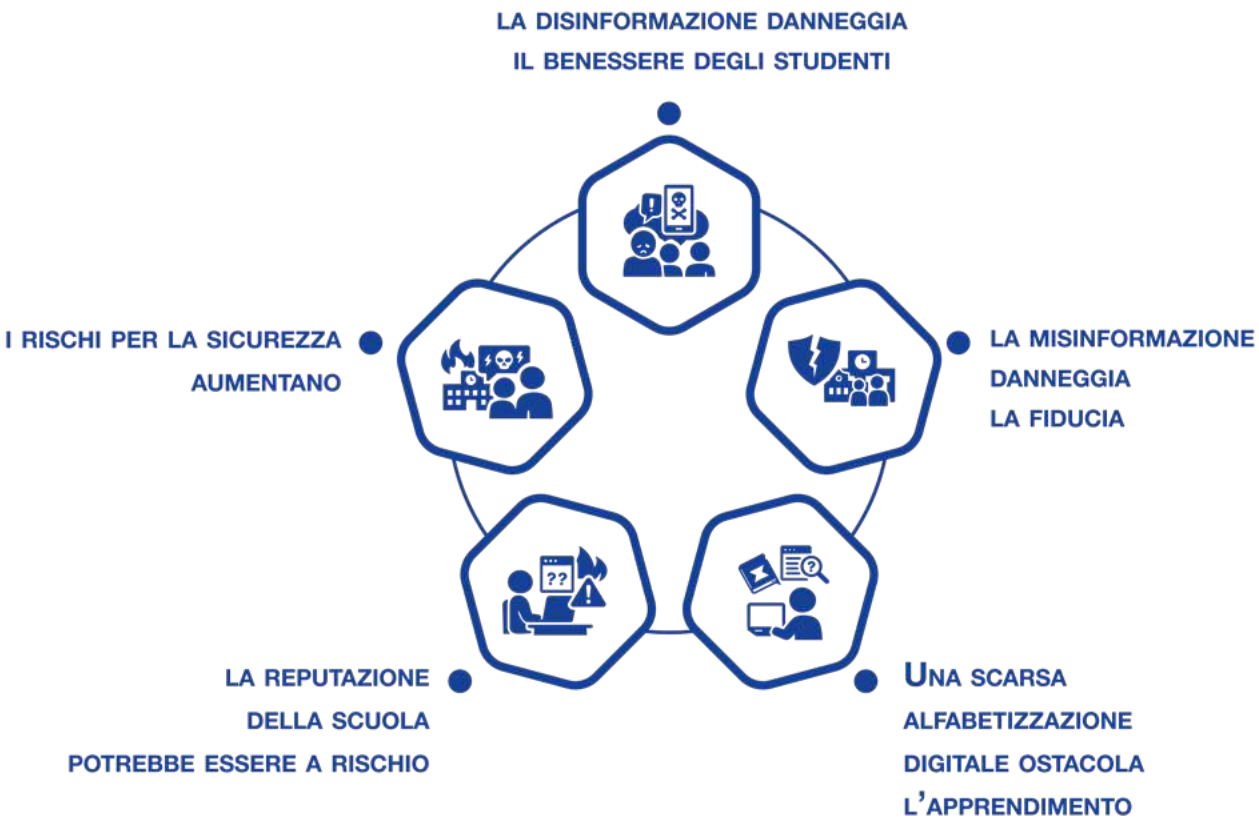
Per i dirigenti, questo aspetto è importante per diversi motivi:

- La disinformazione influisce sul benessere degli studenti. Una notizia falsa che circola sui social media può causare ansia, esclusione o divisione tra gli studenti. I giovani che non sono in grado di distinguere i contenuti affidabili da quelli inaffidabili sono più inclini a sentirsi insicuri o manipolati.

- La disinformazione può danneggiare la fiducia tra le scuole e i genitori. Quando le dicerie si diffondono senza controllo, ad esempio sui cambiamenti dei programmi scolastici, sulle politiche sanitarie o sulle pratiche disciplinari, minano la fiducia nella comunità scolastica.
- Una scarsa alfabetizzazione digitale può compromettere l'apprendimento. Gli studenti che non sono in grado di filtrare le informazioni potrebbero affidarsi a fonti inaffidabili nei loro compiti o introdurre narrazioni dannose nelle discussioni in classe.
- La reputazione della scuola è a rischio. Una singola informazione falsa su una scuola può diffondersi rapidamente online, creando crisi di pubbliche relazioni che distraggono dall'apprendimento e consumano le energie del personale.
- I rischi per la sicurezza aumentano. La disinformazione non riguarda solo notizie fuorvianti, ma include anche challenge dannose, bufale o truffe rivolte ai giovani. Senza alfabetizzazione digitale, gli studenti sono più vulnerabili a questi rischi.

In breve, l'alfabetizzazione digitale non è un lusso per le scuole. È una competenza fondamentale che sta alla base del rendimento scolastico, della coesione della comunità e della sicurezza degli studenti. Riconoscendo questo fatto, i dirigenti possono guidare le loro scuole verso un futuro in cui gli ambienti digitali saranno navigati in modo critico, responsabile e sicuro.

PERCHÉ L'ALFABETIZZAZIONE DIGITALE È IMPORTANTE PER I DIRIGENTI SCOLASTICI



IL RUOLO DEI DIRIGENTI NELLA PROMOZIONE DELL'ALFABETIZZAZIONE DIGITALE

Poiché le sfide digitali toccano ogni aspetto della vita scolastica, promuovere l'alfabetizzazione digitale richiede molto più di qualche lezione sulla sicurezza online. Richiede una leadership sistemica. I dirigenti devono:

1. **Stabilire politiche e procedure chiare.**
   Un approccio che coinvolga l'intera scuola significa integrare l'alfabetizzazione digitale nelle politiche di salvaguardia, nei programmi scolastici e nei codici di condotta. Ciò garantisce aspettative coerenti in tutte le classi, in tutti gli anni scolastici e in tutte le attività extrascolastiche.

2. **Supportare e fornire risorse agli insegnanti.**
   Gli insegnanti sono in prima linea nell'educazione all'alfabetizzazione digitale, ma molti si sentono impreparati. I dirigenti devono garantire l'accesso alla formazione, fornire tempo per lo sviluppo professionale e integrare l'alfabetizzazione digitale nelle priorità didattiche più ampie.

3. **Essere un modello di impegno digitale responsabile.**
   La comunicazione dei dirigenti stessi, sia attraverso newsletter, social media o risposte ai momenti di crisi, dà il tono. Un impegno trasparente, basato su prove concrete e rispettoso mostra agli studenti, al personale e ai genitori come si concretizza nella pratica l'uso critico del digitale.

4. **Costruire partnership con genitori e comunità.**
   L'alfabetizzazione digitale non può essere insegnata in modo isolato a scuola. Genitori e tutori svolgono un ruolo cruciale nel plasmare le abitudini digitali dei giovani. I dirigenti dovrebbero coinvolgere attivamente le famiglie, offrendo workshop, risorse e una comunicazione aperta per allineare gli sforzi tra casa e scuola.

5. **Collaborare con attenzione con i fornitori di tecnologia.**
   Le scuole fanno sempre più affidamento a piattaforme e servizi digitali, dai sistemi di gestione dell'apprendimento alle app didattiche. I dirigenti devono valutare criticamente queste relazioni, assicurandosi che i contratti rispettino la privacy degli studenti e che le piattaforme servano interessi didattici piuttosto che puramente commerciali.

Attraverso questi ruoli, i dirigenti trasformano l'alfabetizzazione digitale da un ideale astratto a una realtà vissuta da studenti e insegnanti.

Ogni volta che rivedete la visione della vostra scuola in materia di alfabetizzazione digitale, confrontatela con le strategie nazionali o regionali in materia di istruzione digitale e protezione dei minori. Ciò garantisce che le iniziative locali rafforzino, anziché duplicare o contraddire, i quadri politici esistenti.

Nel definire le priorità digitali, i dirigenti dovrebbero verificare esplicitamente se gli

strumenti e le pratiche proposti sono coerenti con i valori della scuola, come evidenziato nell'HEADstart #4 dell'ESHA. Ciò significa valutare non solo i vantaggi tecnici, ma anche l'equità, l'inclusione e l'impatto etico a lungo termine di ogni decisione digitale.

SVILUPPO DELLE COMPETENZE E NECESSITÀ DI SUPPORTO: APPROFONDIMENTI DALLA RICERCA DRONE

Il progetto DRONE evidenzia una sfida ricorrente: mentre i dirigenti scolastici riconoscono l'importanza dell'alfabetizzazione digitale, molti si sentono impreparati ad affrontare la complessità delle questioni. Questo divario non è dovuto alla mancanza di impegno, ma al ritmo frenetico del cambiamento. Nuove piattaforme, app e rischi emergono più rapidamente di quanto le politiche e la formazione possano adattarsi.

I risultati dello studio DRONE indicano diverse aree in cui i dirigenti necessitano di particolare supporto:

- Strutture per integrare l'alfabetizzazione digitale nella progettazione dei programmi scolastici. Molti dirigenti desiderano andare oltre le lezioni frammentarie e integrare l'alfabetizzazione digitale in tutte le
materie, ma non dispongono di modelli chiari per farlo.
- Linee guida per rispondere alla disinformazione nella comunità scolastica. I dirigenti spesso si trovano di fronte a dicerie, affermazioni false o contenuti manipolati, ma non sanno come rispondere in modo da placare le tensioni anziché alimentarle.
- Strumenti pratici per supportare gli insegnanti. I dirigenti hanno bisogno di risorse pronte all'uso, moduli di formazione professionale e casi di studio che possano essere adattati al contesto della loro scuola.
- Fiducia nelle proprie competenze digitali. Gli stessi dirigenti a volte hanno difficoltà a valutare
le informazioni online, gestire le comunicazioni sui social media o comprendere le basi della sicurezza informatica. Lo sviluppo professionale dei dirigenti è quindi importante tanto quanto quello degli insegnanti.

La ricerca DRONE suggerisce che una leadership efficace in questo settore richiede umiltà oltre che autorevolezza: riconoscere le lacune nelle proprie competenze, essere disposti ad apprendere insieme al personale e creare una cultura in cui l'alfabetizzazione digitale sia un percorso condiviso.



CASO DI STUDIO: "VOCI NELLA COMUNITÀ"

Una scuola secondaria di medie dimensioni ha affrontato una crisi quando una voce si è diffusa rapidamente sui gruppi dei social media locali. I genitori sostenevano che la scuola intendesse cancellare un popolare programma extracurricolare a causa dei tagli al bilancio. La voce, condivisa da un unico account, ha rapidamente guadagnato terreno e causato rabbia. Il personale ha iniziato a ricevere e-mail frustrate dai genitori e gli studenti temevano di perdere un'attività importante. La dirigente della scuola ha agito rapidamente. Innanzitutto, ha verificato i fatti internamente e ha confermato che non era prevista alcuna cancellazione. Successivamente, ha rilasciato una dichiarazione ufficiale attraverso il sito web della scuola, la newsletter e i canali dei social media. Il messaggio non solo ha chiarito la disinformazione, ma ha anche spiegato come la voce fosse nata da una linea di bilancio interpretata erroneamente in un rapporto pubblico. Infine, ha invitato i genitori a una riunione aperta per discutere in modo trasparente le priorità di finanziamento della scuola.

Questo approccio ha permesso di ottenere tre risultati:

- Ha calmato una crisi, prevenendo ulteriori conflitti.
- Ha ripristinato la fiducia dei genitori, dimostrando che la scuola ha risposto in modo aperto e rispettoso.
- Ha dato l'esempio di un impegno digitale critico, dimostrando agli studenti come rispondere alle informazioni false con prove, chiarezza e dialogo.

Il caso illustra come i dirigenti, agendo in modo deciso e trasparente, possano trasformare una potenziale crisi in un'opportunità di apprendimento e di rafforzamento della fiducia.

CONCLUSIONE

L'alfabetizzazione digitale e la disinformazione non sono questioni secondarie per le scuole, ma sono fondamentali per l'istruzione nel XXI secolo. Per i dirigenti, la responsabilità è duplice: proteggere gli studenti e il personale dai danni causati dalla disinformazione e fornire loro le competenze e la fiducia necessarie per navigare in modo responsabile negli ambienti digitali.

Ciò richiede una leadership proattiva, sistemica e collaborativa. Richiede ai dirigenti di:

- Riconoscere l'impatto di vasta portata dell'alfabetizzazione digitale sull'apprendimento, il benessere e la fiducia.
- Integrare la sicurezza e la competenza digitale nelle politiche, nella cultura e nella pratica quotidiana della scuola.
- Supportare gli insegnanti con formazione, risorse e incoraggiamento.
- Coinvolgere genitori e comunità come partner nell'educazione digitale.
- Sviluppare continuamente le proprie competenze digitali, dando l'esempio dei valori che si desidera trasmettere.

Il progetto DRONE sottolinea che i dirigenti non possono risolvere queste sfide da soli, né devono farlo. Costruendo alleanze, promuovendo l'apertura e abbracciando il loro ruolo di mentori digitali, i dirigenti scolastici possono trasformare le scuole in comunità che non solo resistono alla disinformazione, ma formano anche cittadini informati, resilienti e criticamente impegnati.

CAPITOLO 1

ALFABETIZZAZIONE DELL'INFORMAZIONE

CHE COS'È L'ALFABETIZZAZIONE DELL'INFORMAZIONE?

L'alfabetizzazione informativa e mediale è la capacità di trovare, valutare, interpretare e utilizzare le informazioni in modo efficace. In pratica, significa porsi domande come:

- Chi ha creato queste informazioni e perché?
- Quali prove la supportano?
- Quanto è attuale?
- Quali prospettive o pregiudizi sono presenti?
- Come possono essere applicate queste informazioni in modo responsabile in un contesto scolastico?

In un mondo di messaggi istantanei, post virali e feed basati su algoritmi, l'alfabetizzazione dell'informazione non è più una competenza scolastica facoltativa, ma una competenza fondamentale per la sopravvivenza. Per le scuole, essa è alla base non solo dell'apprendimento in classe, ma anche del benessere degli studenti, della professionalità del personale e della fiducia della comunità.

I dirigenti devono comprendere che il loro ruolo non è semplicemente quello di garantire agli studenti l'accesso alle informazioni. Il loro compito è piuttosto quello di coltivare una cultura di impegno critico a livello scolastico, in cui sia il personale che gli studenti possano mettere in discussione, verificare e applicare le informazioni in modo ponderato ed etico.

SVILUPPARE LA PROPRIA ALFABETIZZAZIONE DELL'INFORMAZIONE COME DIRIGENTE SCOLASTICO

Prima di aiutare gli altri, i dirigenti devono esaminare le proprie competenze. La ricerca del progetto DRONE mostra che molti dirigenti si sentono meno sicuri nel valutare i contenuti online rispetto alla gestione delle politiche scolastiche tradizionali. Il primo passo è l'autovalutazione.

Un test di auto-riflessione

I dirigenti possono chiedersi:

1. Quando leggo una notizia online, controllo automaticamente la fonte?
2. Sono in grado di distinguere tra un articolo basato sui fatti e un articolo di opinione?
3. Sono consapevole dei tratti che caratterizzano immagini manipolate o video "deepfake"?
4. Mi sento sicuro nel rispondere ai genitori o agli studenti che condividono affermazioni false?
5. Quando prendo delle decisioni, mi affido a una serie di fonti affidabili piuttosto che a un unico canale?

Se la risposta sincera a molte di queste domande è "no" o "non sono sicuro", allora la formazione professionale nell'alfabetizzazione informativa non è solo consigliabile, ma urgente.

Misure pratiche per i dirigenti

- Impegnatevi nella formazione: partecipate a corsi online o workshop che sviluppano competenze digitali e di alfabetizzazione informativa.
- Date l'esempio nella verifica dei fatti: condividete con il personale esempi di come avete verificato una notizia o corretto un errore.
- Utilizzate più fonti: quando presentate dati al personale o ai genitori, citate più di una fonte attendibile.
- Rimanete aggiornati: seguite le organizzazioni educative, i siti di verifica dei fatti e i centri di ricerca che monitorano le tendenze della disinformazione.

Confrontate il vostro percorso di apprendimento professionale con i quadri di riferimento nazionali relativi alle competenze degli insegnanti e dei dirigenti in materia di alfabetizzazione digitale o mediatica. L'utilizzo di questi punti di riferimento vi aiuterà a dare priorità alle aree di sviluppo che gli organismi di controllo e i ministeri hanno già evidenziato come strategiche.

SOSTENERE GLI INSEGNANTI NEL PROMUOVERE L'ALFABETIZZAZIONE DELL'INFORMAZIONE

Gli insegnanti sono in prima linea nell'educazione alle competenze digitali. Tuttavia, molti di loro non dispongono di approcci strutturati o non hanno la sicurezza necessaria per integrare l'alfabetizzazione informatica nell'insegnamento quotidiano. I dirigenti possono adottare diverse misure per garantire una pratica coerente ed efficace in tutta la scuola.

Creare un approccio per l'istituto scolastico nel suo complesso

- Integrazione nel programma scolastico: integrare l'alfabetizzazione informatica in più materie, non solo nelle materie relative a ICT. Ad esempio, gli insegnanti di storia possono confrontare le fonti, mentre quelli di scienze possono analizzare le affermazioni sulla salute o sul clima.
- Formazione professionale: offrire sessioni di formazione e risorse sulla valutazione dei contenuti online, l'insegnamento dell'analisi delle fonti e il riconoscimento dei media manipolati.
- Centri di risorse: creare un centro digitale condiviso dove gli insegnanti possano accedere a
strumenti di verifica dei fatti, liste di controllo e programmi didattici.
- Incoraggiamento all'apprendimento tra pari: promuovere la collaborazione tra insegnanti, in modo
che il personale condivida le strategie didattiche che hanno funzionato bene.

Esempio: Giornata di Alfabetizzazione in una Scuola Aperta

Il dirigente di una scuola media inferiore ha organizzato una "Giornata dell'alfabetizzazione digitale" in cui ogni materia ha incorporato un esercizio critico sull'informazione. Le lezioni di matematica includevano l'individuazione di errori nei grafici, quelle di inglese il confronto tra i titoli dei media e quelle di arte l'esame della manipolazione delle immagini. Gli insegnanti hanno segnalato un maggiore coinvolgimento degli studenti e una comprensione più chiara del fatto che mettere in discussione le informazioni è importante in tutte le discipline, non solo nelle lezioni di informatica.

SOSTENERE INDIRETTAMENTE L'ALFABETIZZAZIONE DELL'INFORMAZIONE DEGLI STUDENTI

Sebbene i dirigenti di solito non insegnino quotidianamente, hanno un ruolo importante nel definire le condizioni in cui gli studenti apprendono. Assicurando che i programmi di studio, le risorse e la formazione degli insegnanti siano allineati, i dirigenti consentono agli studenti di:

- Porre domande critiche: "Chi l'ha detto?" "Posso fidarmi?"
- Comparare più punti di vista: riconoscere che fonti diverse possono inquadrare gli eventi in modo diverso.
- Verificare praticamente: imparare a utilizzare siti web di verifica dei fatti, la ricerca inversa delle immagini e database affidabili.
- Sviluppare la consapevolezza etica: comprendere l'impatto della condivisione di contenuti falsi o dannosi.

I dirigenti che creano spazio per queste pratiche garantiscono che l'alfabetizzazione informativa divenga una competenza fondamentale per gli studenti, non un'aggiunta facoltativa.



QUANDO LE COSE VANNO MALE – DALLA SFIDA ALLA CRISI

Nonostante gli sforzi, le scuole dovranno affrontare incidenti in cui una scarsa alfabetizzazione informativa causa disagi o danni.

Scenari comuni

- Dicerie tra gli studenti: un video o un post virale scatena ansia o conflitti a scuola.
- Genitori male informati: le famiglie condividono e agiscono sulla base di informazioni false riguardo l'amministrazione della scuola.
- Problemi con il personale: un insegnante utilizza inconsapevolmente fonti inaffidabili in classe o condivide contenuti non verificati.
- Crisi di reputazione: una notizia fuorviante sulla scuola si diffonde a livello locale o nazionale.

Misure che i dirigenti devono adottare per reagire

1. Verificare rapidamente: raccogliere i fatti prima di rispondere pubblicamente.
2. Comunicare in modo chiaro: condividere le informazioni verificate con studenti, personale e genitori attraverso i canali ufficiali.
3. Educare: utilizzare gli incidenti come opportunità di apprendimento, spiegando come si diffondono le misinformazioni e cosa si può imparare da esse.
4. Sostenere il personale e gli studenti: fornire sostegno emotivo se le misinformazioni hanno causato disagio.
5. Rivedere i protocolli: dopo una crisi, valutare se linee guida più chiare o una formazione più approfondita avrebbero potuto impedire l'aggravarsi della situazione.



CASO DI STUDIO: "IL FALSO AVVISO SANITARIO"

In una scuola secondaria, su WhatsApp è circolata una notizia falsa sulla salute, secondo cui la scuola aveva rilevato un grave focolaio e avrebbe chiuso. Il panico si è diffuso rapidamente tra studenti e genitori e i media locali hanno iniziato a fare domande. Il preside ha agito rapidamente:

- Ha verificato i fatti con le autorità sanitarie locali.
- Ha rilasciato una dichiarazione su tutti i canali ufficiali chiarendo che il messaggio era falso.
- Ha contattato i genitori tramite SMS ed e-mail per rassicurarli direttamente.
- Ha tenuto un'assemblea in cui gli studenti hanno discusso di come si era diffusa la voce e di come avrebbe potuto essere verificata.

Considerando l'incidente non solo come una crisi, ma anche come un'occasione di apprendimento, la scuola ha trasformato il disagio in un'opportunità di crescita. I genitori hanno poi espresso apprezzamento per la comunicazione trasparente e proattiva.

STRUMENTI PRATICI PER I DIRIGENTI

Checklist sull'alfabetizzazione dell'informazione per i dirigenti

- Verificare le informazioni prima di condividerle con il personale, i genitori o gli studenti.
- Essere in grado di identificare almeno tre fonti affidabili per gli aggiornamenti sulle politiche
scolastiche ed educative.
- Nei comunicati, dare l'esempio di un approccio critico alle informazioni.
- Verificare che gli insegnanti della scuola abbiano accesso a risorse e formazione sull'alfabetizzazione informativa.
- Verificare che il nostro programma di studi integri l'alfabetizzazione informativa in tutte le materie.
- Avere un piano chiaro per rispondere alle crisi dovute al diffondersi di disinformazione.

Strumenti e risorse consigliati

- Siti web di verifica dei fatti: Snopes (https://www.snopes.com/), Full Fact (https://fullfact.org/), EU vs Disinfo, (https://euvsdisinfo.eu/) Bufale.net (https://www.bufale.net/) Open Fact Checking (https://www.open.online/c/fact-checking/).
- Ricerca per immagini: Google Immagini (https://images.google.com/), TinEye (https://tineye.com/).
- Risorse per l'alfabetizzazione alle notizie: News Literacy Project, quadro di riferimento dell'UNESCO per l'alfabetizzazione digitale.1
- Strumenti del progetto SAILS: liste di controllo pratiche per la classe e autovalutazioni dell'alfabetizzazione informativa. (https://library.parenthelp.eu/captains-handbook-sails-resource-for-school-leaders/, https://library.parenthelp.eu/seafarers-guide/).

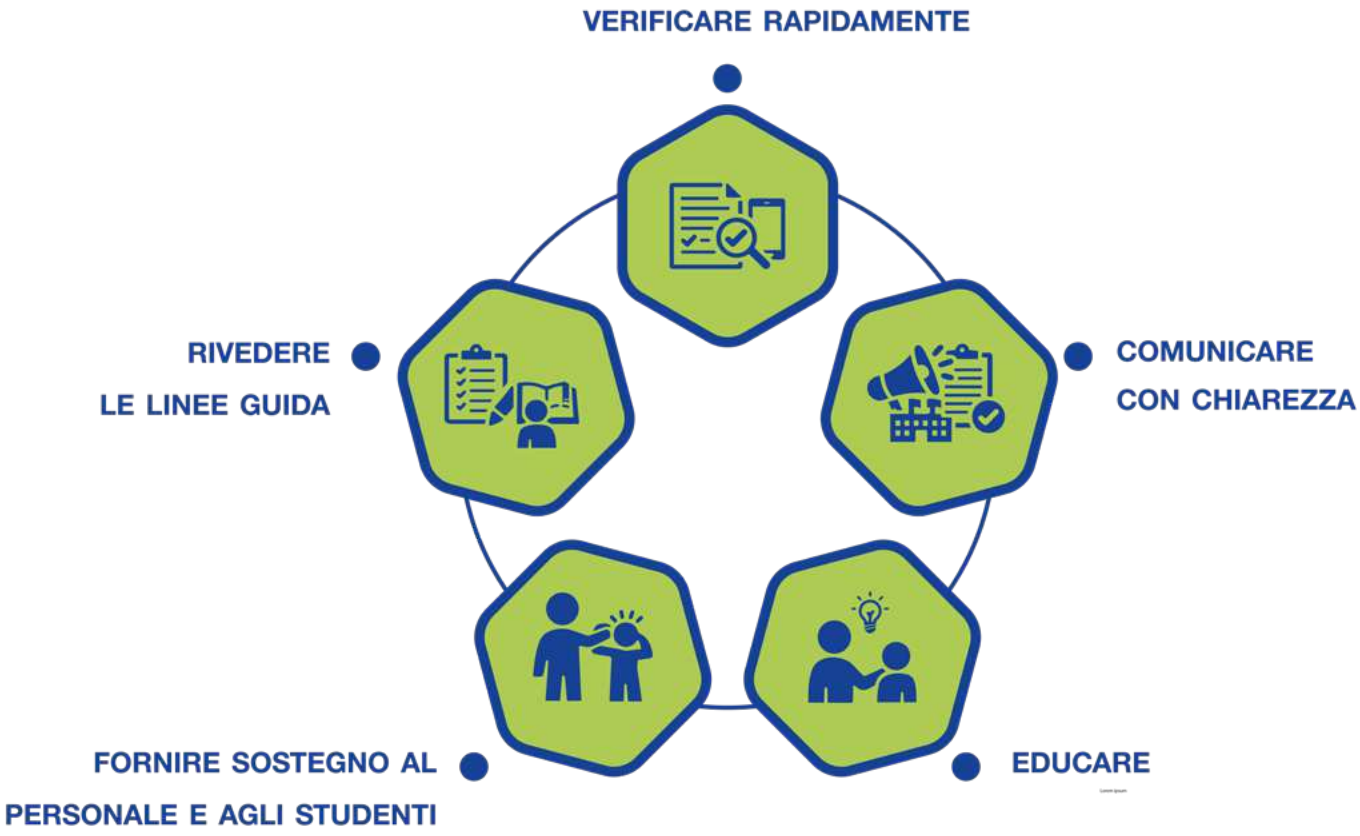
CONCLUSIONE

L'alfabetizzazione informativa non è solo un'altra competenza che gli studenti devono padroneggiare. È il fondamento di una partecipazione sicura, critica e consapevole alla vita digitale. Per i dirigenti, sviluppare l'alfabetizzazione informativa significa:

- Sviluppare le proprie competenze.
- Fornire agli insegnanti formazione e strumenti.
- Integrare l'impegno critico in tutto il programma di studi.
- Rispondere in modo rapido ed efficace quando la disinformazione causa disagi.

Quando i dirigenti promuovono l'alfabetizzazione informativa, non solo proteggono le loro comunità scolastiche dai rischi della disinformazione, ma alimentano anche una cultura in cui la verità, la ricerca e la fiducia sono valori fondamentali. Non si tratta semplicemente di un'azione difensiva, ma di un'azione di leadership che prepara i giovani a prosperare in un mondo incerto e ricco di informazioni.

COME RISPONDERE A UNA SCARSA ALFABETIZZAZIONE DELL'INFORMAZIONE



CAPITOLO 2

DISINFORMAZIONE, MISINFORMAZIONE E FAKE NEWS

COMPRENDERE LA DISINFORMAZIONE, LA MISINFORMAZIONE E LE FAKE NEWS

Sebbene spesso utilizzati in modo intercambiabile, i termini disinformazione, misinformazione e fake news descrivono fenomeni distinti:

- **Misinformazione**: informazioni false o fuorvianti condivise senza intenzioni dannose. Esempio: un genitore che inoltra un post virale su una "nuova politica sui compiti a casa" che ritiene vera ma che in realtà non lo è.
- **Disinformazione**: informazioni false create e condivise deliberatamente per causare danni, manipolare opinioni o minare la fiducia. Esempio: una campagna coordinata che diffonde notizie false sui risultati di una scuola per screditare la sua dirigenza.
- **Fake News**: termine colloquiale usato in senso lato per descrivere storie inventate presentate come notizie reali. Può includere sia la disinformazione sia la misinformazione.

Nel contesto scolastico, queste questioni non sono astratte. Influiscono sul benessere degli studenti, sulla fiducia della comunità, sul morale del personale e sulla reputazione dell'istituzione. I dirigenti scolastici devono comprendere in modo approfondito come circolano queste forme di informazioni false e come reagire.

Perché è importante per i dirigenti

La disinformazione e la cattiva informazione hanno un impatto sulle scuole a diversi livelli:

1. Per gli studenti:
   - L'esposizione a contenuti online fuorvianti o dannosi può distorcere la loro visione del mondo.
   - Le bufale virali possono causare paura (ad esempio, "challenge pericolose") o incoraggiare comportamenti rischiosi.
   - Le false accuse nei confronti dei compagni o degli insegnanti possono alimentare il bullismo o l'esclusione sociale.
2. Per i genitori e la comunità:
   - La misinformazione sulle politiche scolastiche (ad esempio, programmi didattici, norme sanitarie o finanziamenti) può scatenare rabbia o ansia inutili.
   - Le notizie false possono minare la fiducia tra le famiglie e la scuola.
3. Per il personale e la dirigenza:
   - Gli insegnanti potrebbero inavvertitamente condividere informazioni false con gli studenti.
   - I dirigenti possono essere presi di mira direttamente da campagne di disinformazione che mettono in discussione la loro competenza o le loro decisioni.
   - Il danno alla reputazione può diffondersi rapidamente online, creando situazioni di crisi.

Per questi motivi, affrontare la disinformazione non significa solo proteggere gli studenti, ma è una responsabilità della dirigenza che si estende alla comunicazione, all'amministrazione e alla costruzione della comunità scolastica.

SVILUPPARE LE CAPACITÀ DEI DIRIGENTI NEL RICONOSCERE LE FAKE NEWS

I dirigenti non possono essere un modello di resilienza o sostenere gli insegnanti se non hanno fiducia nella propria capacità di riconoscere la disinformazione. Una base solida inizia con lo sviluppo delle competenze personali.

Domande chiave da porsi quando si valutano le informazioni

1. Fonte: chi ha pubblicato questa informazione? La fonte è credibile?
2. Scopo: è stato creato per informare, persuadere, intrattenere o ingannare?
3. Prove: il contenuto cita dati affidabili o si basa su emozioni e aneddoti?
4. Attualità: è recente? Le notizie vecchie vengono spesso riciclate come “attuali”.
5. Verifica: queste informazioni possono essere verificate incrociandole con altre fonti attendibili?
6. Linguaggio e tono: utilizza un linguaggio drammatico, sensazionalistico o divisivo per suscitare emozioni?

Azioni pratiche per i leader

- Mettetevi alla prova regolarmente: utilizzate giochi online e strumenti di formazione (ad esempio, “Bad News” di DROG, che simula le tattiche di disinformazione - https://www.getbadnews.com/en/play - disponibile in molte lingue).
- Seguite i fact-checker: iscrivitevi alle newsletter di organizzazioni affidabili come Full Fact (https://fullfact.org/), Snopes (https://www.snopes.com/), EU vs Disinfo (https://euvsdisinfo.eu/), Bufale.net (https://www.bufale.net/) o Open Fact Checking (https://www.open.online/c/fact-checking/)
- Rimanete aggiornati: seguite le autorità educative nazionali o locali per ottenere indicazioni verificate ed evitare di affidarvi a dicerie non confermate.

Migliorando il proprio impegno critico, i dirigenti possono agire con sicurezza quando si trovano di fronte a informazioni discutibili.

Quando si elaborano linee guida a livello di istituto scolastico sulla disinformazione, è opportuno allineare le procedure alle linee guida nazionali in materia di alfabetizzazione mediatica o comunicazione strategica emanate per le scuole. Il riferimento a tali documenti rende più facile per personale e genitori comprendere che l’approccio adottato segue standard riconosciuti.

AIUTARE GLI INSEGNANTI A IDENTIFICARE E AFFRONTARE LE FAKE NEWS

Gli insegnanti sono spesso i primi a imbattersi nella disinformazione in classe. Gli studenti possono ripetere dicerie che vedono su TikTok, citare siti web dubbi nei compiti o condividere immagini manipolate nelle chat di gruppo. I dirigenti scolastici devono fornire agli insegnanti le strategie e la sicurezza necessarie per rispondere.

Strategie per i dirigenti a sostegno degli insegnanti

1. Workshop di formazione: offrire sessioni regolari su come identificare la misinformazione, compresi esercizi pratici con esempi reali.

2. Fornire risorse: sviluppare o condividere checklist, strumenti di verifica dei fatti e linee guida da utilizzare durante le lezioni.

3. Creare spazi sicuri: incoraggiare gli insegnanti a discutere apertamente delle difficoltà. Il personale dovrebbe sentirsi libero di ammettere: “Non sono sicuro che questo sia vero, controlliamo insieme”.

4. Incoraggiare l’integrazione tra le materie: l’alfabetizzazione informativa non dovrebbe essere relegata nell’ambito delle ICT. Le lezioni di scienze, storia e persino arte offrono l’opportunità di valutare criticamente fonti e immagini.

Esempio: pacchetto di risorse per la classe

Un dirigente scolastico ha collaborato con gli insegnanti per creare un “Kit di strumenti per investigare le fonti”, che includeva:

- Un diagramma di flusso con domande per valutare le fonti.
- Link a siti web di verifica dei fatti adatti ai più giovani.
- Esempi di compiti che premiano le domande critiche, non solo le risposte corrette.

Gli insegnanti hanno riferito di aver maturato una maggiore fiducia; gli studenti, di essere diventati più riflessivi riguardo alle fonti utilizzate nei progetti.

REAGIRE QUANDO LE COSE VANNO MALE

Nonostante le misure proattive, gli episodi di disinformazione continueranno a verificarsi. Ciò che conta è come reagiscono le scuole.

Misure per i dirigenti in situazioni di crisi

1. Verificare rapidamente: accertate i fatti prima di rispondere pubblicamente.
2. Comunicare in modo trasparente: condividete le informazioni verificate attraverso i canali ufficiali della scuola (sito web, newsletter, app per i genitori).
3. Coinvolgere direttamente: se i genitori sono preoccupati, organizzate una riunione o una sessione di domande e risposte per affrontare apertamente le dicerie.
4. Sostenete il personale: se un insegnante è stato screditato dalla disinformazione, sostenetelo sia in pubblico che in privato.
5. Educare la comunità: utilizzate l'incidente come opportunità didattica per studenti e personale su come si diffonde la disinformazione.

Misure preventive a lungo termine

- Stabilite un "protocollo di risposta alle dicerie" in modo che il personale sappia come segnalare rapidamente i problemi.
- Formate il personale alla comunicazione di crisi per garantire messaggi coerenti e rassicuranti.
- Costruite partnership con i media locali e i gruppi di genitori, in modo che esistano canali affidabili per chiarire le questioni.



CASO DI STUDIO: "LA CONTROVERSIA SUL PROGRAMMA SCOLASTICO"

Una scuola secondaria ha introdotto un nuovo modulo di educazione civica incentrato sull'alfabetizzazione informativa e mediale. Quasi immediatamente, nella comunità hanno iniziato a diffondersi false affermazioni: alcuni genitori sono stati informati (tramite un post virale su Facebook) che la scuola stava "indottrinando" gli studenti con opinioni politiche. Nel giro di pochi giorni, l'ufficio della scuola è stato sommerso da e-mail e telefonate rabbiose. Alcuni genitori hanno minacciato di ritirare i propri figli.

Risposta della Dirigenza

- Il dirigente ha rilasciato una dichiarazione chiara e basata su prove concrete in cui spiegava le modifiche al programma scolastico, includendo link al quadro educativo deciso dalla scuola sulla base dei programmi ministeriali.
- È stata organizzata una serata informativa per i genitori, durante la quale gli insegnanti hanno presentato in modo trasparente i contenuti delle lezioni e hanno affrontato direttamente le preoccupazioni dei genitori.
- Durante le assemblee, gli studenti hanno discusso di come si era diffusa la voce e dell'importanza di verificare le fonti.

Risultato

La risposta proattiva ha calmato le tensioni. I genitori hanno apprezzato la trasparenza, il personale si è sentito supportato e gli studenti hanno imparato in prima persona come la disinformazione possa distorcere la realtà. L'incidente è diventato un'opportunità didattica piuttosto che una crisi.

STRUMENTI PRATICI PER I DIRIGENTI

Lista dei segnali di allarme relativi alla disinformazione

- La notizia non ha un autore o una fonte chiari. ☐
- Il linguaggio è emotivo, sensazionalistico o divisivo. ☐
- Il contenuto non può essere verificato da almeno un'altra fonte credibile. ☐
- Le immagini o i video possono apparire alterati o privi di contesto. ☐
- La notizia viene condivisa principalmente su gruppi privati o account anonimi. ☐

Lista di controllo delle azioni per i dirigenti

- Ho formato il personale a riconoscere la misinformazione e la disinformazione. ☐
- La nostra scuola ha un piano di comunicazione chiaro per rispondere alle dicerie. ☐
- I genitori sanno come accedere alle informazioni verificate dalla scuola. ☐
- Ho integrato la valutazione critica delle fonti in diverse materie. ☐
- Nel mio ruolo di dirigente, do l'esempio di una comunicazione digitale responsabile. ☐

Letture e risorse consigliate

- UNESCO: programma di alfabetizzazione mediatica e informativa per insegnanti.2
- News Literacy Project: risorse didattiche e guide gratuite. 3
- Full Fact (Regno Unito) (https://fullfact.org/), Snopes (Stati Uniti) (https://www.snopes.com/), EU vs Disinfo (Europa) (https://euvsdisinfo.eu/): organizzazioni affidabili per la verifica dei fatti.
- Il gioco "Bad News" di DROG: una risorsa interattiva che aiuta i giocatori a comprendere le strategie di disinformazione (https://www.getbadnews.com/en/play), disponibile in molte lingue.

CONCLUSIONE

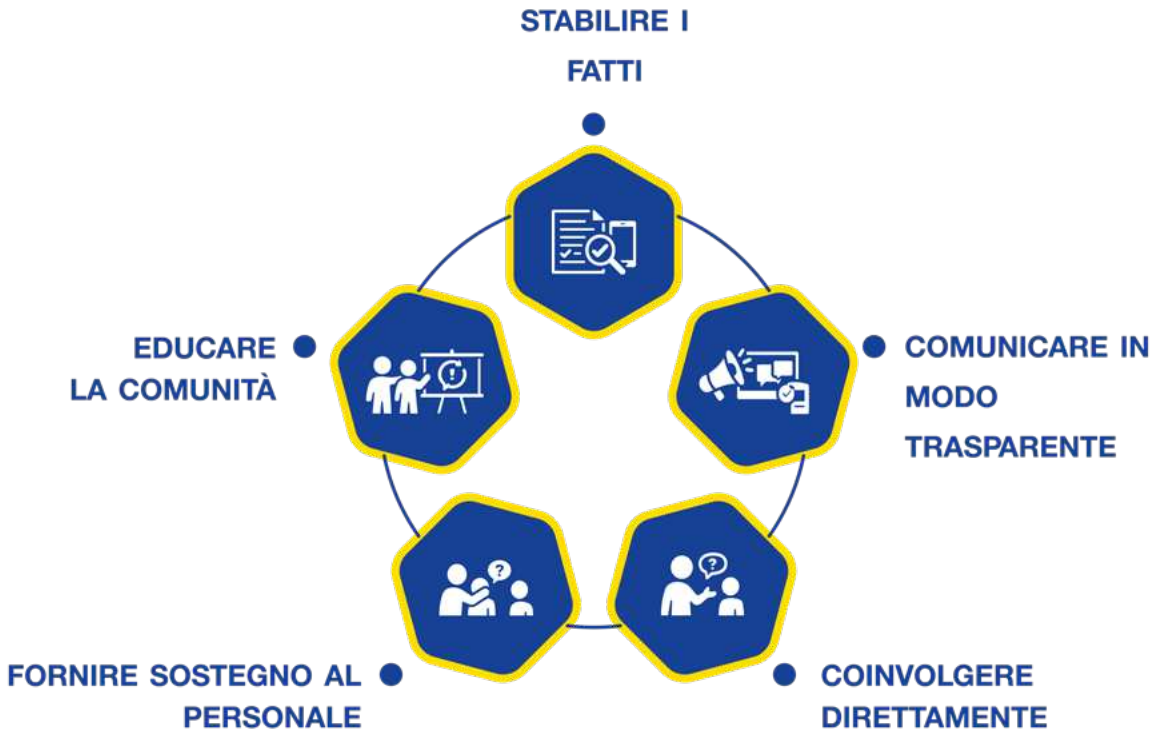
La disinformazione, la misinformazione e le fake news non sono problemi esterni che riguardano solo il mondo esterno. Raggiungono direttamente i corridoi delle scuole, le aule e le comunità. Per i dirigenti, il compito è duplice: proteggere la comunità scolastica dai danni e fornire agli studenti e al personale le competenze necessarie per navigare negli ambienti digitali.

Ciò richiede ai dirigenti di:

- Rafforzare le proprie competenze nel riconoscere e rispondere alle fake news.
- Fornire agli insegnanti formazione, strumenti e fiducia.
- Comunicare in modo trasparente con i genitori e le comunità.
- Sviluppare la resilienza in modo che la disinformazione diventi un'opportunità di crescita, non di crisi.

Adottando queste misure, i dirigenti non solo affrontano i rischi immediati, ma adempiono anche a una missione educativa più profonda: preparare i giovani a vivere come cittadini informati, critici e responsabili in un mondo in cui spesso la verità stessa è contestata.

MISURE PER DIRIGENTI IN UNA SITUAZIONE DI CRISI



CAPITOLO 3

COSTRUIRE LA RESILIENZA

PERCHÉ LA RESILIENZA È IMPORTANTE NELL' ERA DIGITALE

La resilienza è spesso descritta come la capacità di riprendersi rapidamente dalle difficoltà o dalle battute d'arresto. Nell'era digitale, la resilienza include anche la capacità di resistere a contenuti dannosi, manipolazioni online e alle pressioni in rapida evoluzione dei social media. Per le scuole, la resilienza non è solo una caratteristica individuale, ma anche una capacità collettiva.

- Per gli studenti, resilienza significa la capacità di fronteggiare l'esposizione a mode online dannose, cyberbullismo o fake news senza danni a lungo termine per il proprio benessere.
- Per gli insegnanti, resilienza significa capacità di adattarsi a nuove sfide, tra cui molestie online, rapidi cambiamenti tecnologici o crisi dovute al diffondersi della disinformazione nelle loro classi.
- Per i dirigenti, la resilienza implica la gestione delle difficoltà istituzionali con calma e lungimiranza, assicurando che, quando sorgono problemi, la comunità scolastica sia in grado di rispondere in modo costruttivo piuttosto che reattivo.

La ricerca DRONE sottolinea che la resilienza non è innata. È una competenza che si può apprendere e che può essere rafforzata attraverso politiche scolastiche deliberate, modelli di leadership e pratiche collettive.

COSTRUIRE LA PROPRIA RESILIENZA COME DIRIGENTE

La leadership nell'era digitale è impegnativa. La disinformazione, gli incidenti informatici e i conflitti all'interno della comunità scolastica possono mettere alla prova anche i dirigenti più esperti. Lo sviluppo della resilienza inizia con la consapevolezza di sé e le strategie personali.

Domande di autovalutazione per dirigenti

1. Riesco a mantenere la calma sotto pressione o mi sento sopraffatto quando emergono crisi legate al mondo digitale?

2. Sono sicuro di riuscire a separare i fatti dalle emozioni quando rispondo alle dicerie che circolano online?

3. Ho strategie personali (ad esempio, reti di supporto tra pari, pratiche di riflessione) per gestire lo stress?

4. Do l'esempio con risposte costruttive quando mi trovo di fronte a disinformazione o ostilità online?

Pratiche di resilienza personale

- Stabilire dei limiti alle informazioni: evitare di reagire immediatamente a ogni messaggio o voce. Prendersi il tempo necessario per verificare e consultarsi prima di rispondere.
- Utilizzare le reti professionali: creare supporto reciproco tra gli altri dirigenti per condividere strategie ed esperienze.
- Dare priorità al benessere: assicuratevi di avere delle routine (esercizio fisico, riposo, consapevolezza) che mantengano l'equilibrio mentale. Un dirigente stressato fatica a prendere decisioni con calma.
- Dare l'esempio in termini di resilienza: gli studenti e il personale notano come reagiscono i dirigenti. La vostra risposta calma e misurata dà il tono all'intera comunità.

SOSTENERE GLI INSEGNANTI NELLA COSTRUZIONE DELLA RESILIENZA

Gli insegnanti sono in prima linea nelle sfide digitali. Possono essere esposti al cyberbullismo da parte di studenti, a molestie online da parte dei genitori o a richieste eccessive di gestione delle nuove tecnologie. I dirigenti devono sostenere attivamente il personale nello sviluppo della resilienza.

Azioni di leadership

1. Sviluppo professionale: offrite formazione sulle strategie di gestione dello stress digitale, compresa la gestione dei messaggi ostili e la protezione dei confini professionali online.

2. Politiche chiare: assicurarsi che il personale sappia quali misure adottare se viene preso di mira online (ad esempio, segnalare alla leadership, documentare gli incidenti, coinvolgere le autorità se necessario).

3. Equilibrio del carico di lavoro: le iniziative digitali non devono sovraccaricare il personale. I dirigenti devono garantire che la tecnologia migliori l'apprendimento anziché creare inutili stress amministrativi.

4. Programmi di benessere: integrare la resilienza nei programmi di benessere del personale, sottolineando che chiedere aiuto è un punto di forza, non una debolezza.

Verificate come vengono definiti la resilienza, la salute mentale e la sicurezza online nella normativa nazionale in materia di istruzione o benessere dei minori e utilizzate la stessa terminologia nei documenti della vostra scuola. Questo linguaggio comune aiuta i servizi esterni e le autorità a collaborare agevolmente con la vostra scuola quando sorgono dei problemi.

Esempio: molestie online nei confronti degli insegnanti

In una scuola, un insegnante è stato oggetto di scherno anonimo su un account social gestito dal corpo studentesco. Il dirigente ha agito rapidamente, rassicurando l'insegnante sul fatto che la dirigenza avrebbe affrontato la questione con serietà, coinvolgendo i genitori e collaborando con la piattaforma per rimuovere il contenuto. L'insegnante ha ricevuto sostegno emotivo dai colleghi e indicazioni su come proteggere la propria presenza digitale professionale. L'incidente ha rafforzato l'importanza che i dirigenti creino una cultura di tolleranza zero nei confronti delle molestie online.

SVILUPPARE LA RESILIENZA TRA GLI STUDENTI

Gli insegnanti sono in prima linea nelle sfide digitali. Possono essere esposti al cyberbullismo da parte di studenti, a molestie online da parte dei genitori o a richieste eccessive di gestione delle nuove tecnologie. I dirigenti devono sostenere attivamente il personale nello sviluppo della resilienza.

Strategie per la resilienza degli studenti

- Inserire la resilienza digitale nel programma scolastico: le lezioni dovrebbero includere strategie di gestione, non solo avvertimenti sui rischi.
- Creare meccanismi di segnalazione sicuri: assicurarsi che gli studenti sappiano che possono segnalare esperienze online dannose senza timore di punizioni.
- Promuovere il sostegno tra pari: incoraggiare i supervisori o i mentori degli studenti a sostenere i compagni che affrontano sfide digitali.
- Concentrarsi sulle competenze emotive: aiutare gli studenti a comprendere i fattori emotivi, a gestire lo stress e riflettere prima di reagire online.

Esempio pratico: workshop per studenti

Una scuola ha introdotto un workshop dal titolo “Rifletti prima di pubblicare”, che insegna agli studenti come rallentare, riflettere e verificare prima di rispondere a contenuti provocatori online. Il workshop ha utilizzato scenari di role-play e discussioni di gruppo. Gli studenti hanno poi riferito di sentirsi più sicuri nel resistere alla pressione dei coetanei che li spingeva no a condividere contenuti dannosi o falsi.

QUANDO LE COSE VANNO MALE: DALLE DIFFICOLTÀ ALLE CRISI

La resilienza viene messa alla prova soprattutto nei momenti di crisi. Le scuole possono trovarsi ad affrontare situazioni come:

- Una sfida virale dannosa che incoraggia comportamenti rischiosi.
- Bullismo online rivolto agli studenti o al personale scolastico.
- Rabbia della comunità alimentata dalla disinformazione.
- Una violazione dei dati che espone le informazioni degli studenti.

Struttura di risposta del leader: le "4 C"

1. Calma: non alimentate il panico. Mostrate compostezza e prendete decisioni ponderate.
2. Chiarezza: comunicate in modo trasparente le informazioni verificate.
3. Cura: date priorità al benessere degli studenti e del personale, offrendo consulenza o supporto pratico ove necessario.
4. Comunità: coinvolgete i genitori, le autorità locali e esperti esterni per creare una risposta unitaria.

Esempio: sfida virale online

In una grande scuola secondaria, gli studenti sono stati presi dal panico a causa di una "sfida pericolosa" virale che circolava su TikTok. Si sono diffuse dicerie secondo cui alcuni studenti avrebbero tentato di affrontarla. Il dirigente ha convocato una task force di crisi, ha verificato che nessuno studente fosse stato coinvolto direttamente e ha rilasciato una dichiarazione chiara ai genitori spiegando la situazione. Durante le assemblee, agli studenti è stato insegnato come si diffondono le bufale virali e come resistere alla pressione dei coetanei La scuola ha fornito assistenza psicologica a coloro che si sentivano angosciati. La risposta proattiva ha impedito l'isteria e rafforzato la fiducia della comunità nella leadership.

CREARE UNA CULTURA ORGANIZZATIVA SCOLASTICA RESILIENTE

La resilienza non riguarda solo gli individui, ma deve essere integrata nei sistemi e nella cultura organizzativa della scuola.

Azioni chiave per i dirigenti

- Integrazione delle azioni amministrative: rendere la resilienza parte integrante delle azioni amministrative, di salvaguardia del comportamento e del benessere.
- Esercitazioni regolari: proprio come le scuole praticano esercitazioni antincendio, prendere in considerazione “esercitazioni di incidenti digitali” in cui il personale e gli studenti provano le risposte alla disinformazione o al cyberbullismo.
- Riconoscimenti e premi: celebrare gli esempi di resilienza tra il personale e gli studenti (ad esempio, riconoscendo uno studente che ha resistito con calma alla pressione dei coetanei che lo spingevano a condividere contenuti dannosi).
- Coinvolgimento della comunità: collaborare con i genitori, le organizzazioni locali e i servizi di salute mentale per creare una rete di sostegno più ampia.

STRUMENTI PRATICI PER I DIRIGENTI

Checklist sulla resilienza per dirigenti

- Ho strategie per gestire il mio stress durante le crisi digitali. ☐
- Il personale ha accesso a politiche chiare e formazione sulla resilienza. ☐
- Agli studenti vengono insegnate competenze di resilienza emotiva e digitale durante le lezioni. ☐
- Disponiamo di sistemi sicuri per segnalare i danni digitali. ☐
- Il nostro piano di comunicazione di crisi dà priorità alla calma, alla chiarezza, all'attenzione e alla comunità. ☐
- I genitori sono coinvolti come partner alla pari nel sostenere la resilienza. ☐

Risorse consigliate

- UK Safer Internet Centre: risorse sulla resilienza e la sicurezza online.[1]
- UNICEF: Linee guida sul benessere digitale per bambini e scuole.[2]
- Ditch the Label: organizzazione che offre risorse sul bullismo online e sulla resilienza.[3]
- Strumenti del progetto SAILS: esercizi pratici per valutare le risposte emotive ai contenuti online

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

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

3 https://ditchthelabel.org/

CONCLUSIONE

La resilienza nelle scuole non significa prevenire ogni crisi o proteggere gli studenti da ogni pericolo. Significa sviluppare la capacità di reagire in modo costruttivo quando si presentano delle sfide. Per i dirigenti, ciò comporta:

- Sviluppare le proprie pratiche di resilienza.
- Supportare gli insegnanti nell'affrontare lo stress digitale e le molestie.
- Integrare lo sviluppo della resilienza degli studenti nel programma scolastico e nella cultura organizzativa della scuola.
- Gestire le risposte alle crisi dando l'esempio di calma, chiarezza, attenzione e senso di comunità.

Quando le scuole sviluppano la resilienza come competenza condivisa, non solo diventano più sicure e preparate, ma anche più sicure di sé. I dirigenti che danno priorità alla resilienza preparano le loro scuole alle incertezze di un mondo digitale in rapida evoluzione e forniscono agli studenti la capacità permanente di affrontare le sfide con forza e consapevolezza critica.

QUADRO DI RISPOSTA PER I LEADER: LE “4 C”



CAPITOLO 4

PROBLEM-SOLVING

PERCHÉ LA RISOLUZIONE DEI PROBLEMI È IMPORTANTE NELL'ERA DIGITALE

Le scuole hanno sempre dovuto affrontare difficoltà, dalle dispute nel cortile della ricreazione ai cambiamenti nei programmi scolastici. Ma nell'era digitale, i problemi spesso sorgono all'improvviso, si diffondono rapidamente e hanno impatti imprevedibili. Un singolo post fuorviante può scatenare una apprensione diffusa. Un guasto al software può interrompere l'apprendimento di centinaia di studenti. Un episodio di cyberbullismo può degenerare in una crisi che coinvolge genitori, media e autorità.
Una risoluzione efficace dei problemi non è quindi solo una caratteristica utile della leadership. È una competenza fondamentale per i dirigenti che devono bilanciare esigenze contrastanti, risolvere conflitti e guidare il personale e gli studenti attraverso complessi dilemmi digitali.

La ricerca DRONE sottolinea che la risoluzione dei problemi digitali richiede tre capacità fondamentali:

1. Pensiero critico: identificare il vero problema al di là delle apparenze.
2. Creatività: generare soluzioni multiple, non solo soluzioni rapide.
3. Fiducia: agire con determinazione, anche sotto pressione.

SVILUPPARE CAPACITÀ DI RISOLUZIONE DEI PROBLEMI IN QUANTO DIRIGENTE

Prima di dare indicazioni a insegnanti o studenti e supervisionarli, i dirigenti devono rafforzare le proprie capacità di risoluzione dei problemi.

Un quadro di riferimento riflessivo: il metodo "STOP"

- S – Slow Down (Rallenta): resistete all'impulso di reagire impulsivamente alle dicerie online o agli incidenti digitali.
- T – Think Clearly (Pensa con chiarezza): definite il problema reale. Si tratta di un problema di disinformazione, di un guasto tecnico o di una rottura dei rapporti?
- O – Opzioni: riflettete sulle possibili soluzioni. Coinvolgete il personale quando opportuno.
- P – Pianificate e procedete: scegliere l'opzione più efficace, comunicarla chiaramente e portarla a termine.

Domande di autovalutazione per i dirigenti

1. Tendo ad agire rapidamente senza prima verificare le informazioni?
2. Mi sento a mio agio nel chiedere consiglio agli altri o cerco di risolvere i problemi da solo?
3. Incoraggio approcci creativi o mi attengo rigidamente alle procedure standard?
4. Riesco a mantenere la calma quando i genitori, il personale o gli studenti mi mettono sotto pressione per ottenere risposte immediate?

Riflettendo su queste domande, i dirigenti possono identificare i propri punti di forza e di debolezza nella risoluzione dei problemi digitali.

SOSTENERE GLI INSEGNANTI NELLA RISOLUZIONE DEI PROBLEMI E NEL PROCESSO DECISIONALE

Gli insegnanti si trovano spesso di fronte a dilemmi digitali:

- Uno studente cita informazioni false in un compito.
- Una chat di gruppo online diventa tossica.
- Un genitore invia un'e-mail chiedendo risposte immediate su una notizia che circola.

Senza sostegno, gli insegnanti potrebbero sentirsi sopraffatti o agire in modo incoerente nelle loro risposte. I dirigenti possono rafforzare la capacità degli insegnanti di risolvere i problemi in diversi modi:

Azioni di leadership

1. Formazione professionale: offrire workshop sui dilemmi digitali, utilizzando scenari di vita reale e giochi di ruolo.

2. Protocolli condivisi: sviluppare linee guida a livello scolastico (ad esempio, come segnalare casi di disinformazione, cyberbullismo o molestie online).

3. Empowerment: dare agli insegnanti l'autonomia di prendere decisioni all'interno di quadri chiari, in modo che si sentano sicuri nel gestire questioni minori senza ricorrere sempre all'intervento della dirigenza.

4. Apprendimento tra pari: creare spazi in cui gli insegnanti condividono "storie di risoluzione dei problemi": cosa hanno affrontato, come hanno reagito e cosa hanno imparato.

Rivedere le procedure di risposta alle crisi alla luce delle normative nazionali e locali in materia di emergenza o gestione dei rischi per le scuole. Citare esplicitamente queste normative nelle linee guida per il personale rassicura la comunità sul fatto che le decisioni nelle crisi digitali si fondano su basi legali e professionali riconosciute.

Esempio: formazione del personale su scenari ipotetici

Il preside di una scuola ha introdotto dei "dilemmi digitali" mensili durante le riunioni del personale. Un mese, gli insegnanti hanno simulato una risposta a un genitore che aveva inoltrato un articolo pieno di teorie complottistiche sulla scuola. Un altro mese, hanno discusso di un account Instagram falso creato da uno studente. Gli insegnanti hanno riferito di sentirsi molto più preparati ad affrontare problemi reali dopo aver provato le risposte in un ambiente sicuro.

COSTRUIRE UNA CULTURA DELLA RISOLUZIONE DEI PROBLEMI PER STUDENTI

Gli studenti hanno bisogno di una guida esplicita nella risoluzione dei problemi. La vita online li pone quotidianamente di fronte a delle scelte: condividere contenuti, rispondere al bullismo o credere a una notizia non verificata. Senza una pratica strutturata, potrebbero affidarsi alle emozioni o all'influenza dei coetanei invece che al ragionamento critico.

Strategie per la risoluzione dei problemi da parte degli studenti

- Apprendimento basato sull'indagine: porre domande aperte che richiedono agli studenti di valutare i contenuti digitali e proporre soluzioni.
- Sfide di gruppo: creare attività in classe in cui gli studenti risolvano collaborativamente problemi digitali effettivi.
- Strumenti decisionali: insegnare semplici schemi come "Fermati, pensa, controlla, agisci" per valutare le scelte online.
- Pratica riflessiva: dopo incidenti digitali, guidare gli studenti a riflettere su cosa è andato storto, quali scelte erano disponibili e cosa potrebbero fare diversamente la prossima volta.

Esempio: progetto di decisione digitale

Una scuola media ha introdotto un progetto in cui gli studenti hanno studiato le challenge virali online. In gruppi, hanno ricercato come si è diffusa la challenge, perché le persone hanno partecipato e quali rischi comportava. Gli studenti hanno poi creato delle presentazioni su alternative più sicure. Questo ha trasformato una moda pericolosa in un esercizio di apprendimento strutturato nella risoluzione dei problemi digitali.

QUANDO LE COSE VANNO MALE: DALLE DIFFICOLTÀ ALLE CRISI

Anche con sistemi solidi, le scuole dovranno affrontare crisi impreviste. La chiave non è evitare ogni problema, ma rispondere in modo costruttivo quando questi si aggravano.

Crisi digitali frequenti

- Una sfida virale dannosa che incoraggia comportamenti rischiosi.
- Bullismo online rivolto a studenti o personale scolastico.
- Rabbia della comunità alimentata dalla disinformazione.
- Una violazione dei dati che espone le informazioni degli studenti.

Struttura di risposta alle crisi per i leader

1. Identificate il problema principale: eliminate il rumore e le emozioni per individuare il problema reale.

2. Riunite le persone chiave: coinvolgete il personale competente (responsabile ICT, responsabile della sicurezza, addetto alle comunicazioni).

3. Decidete rapidamente ma con saggezza: valutate i rischi e scegliete l'opzione meno dannosa.

4. Comunicate in modo chiaro: condividete gli aggiornamenti con il personale, gli studenti e i genitori utilizzando un linguaggio accessibile.

5. Riflettete e valutate: dopo la risoluzione, analizzate cosa ha funzionato e cosa può essere migliorato.



CASO DI STUDIO: "L'ACCOUNT HACKERATO"

In una scuola secondaria, l'account ufficiale dei social media è stato hackerato e utilizzato per pubblicare contenuti offensivi. Nel giro di un'ora, gli screenshot hanno iniziato a circolare tra genitori, studenti.

Risposta della direzione

- Il preside ha immediatamente contattato il team ICT per mettere in sicurezza l'account e rimuovere i post.
- È stata rilasciata una dichiarazione ai genitori in cui si spiegava che l'account era stato compromesso e che era in fase di ripristino.
- Sono state contattate la polizia e l'azienda fornitrice della piattaforma.
- L'incidente è stato successivamente utilizzato nelle assemblee per insegnare agli studenti la sicurezza delle password e la responsabilità digitale.

Risultato

Sebbene la crisi fosse inizialmente dannosa, la risposta trasparente e rapida ha rassicurato i genitori, ripristinato la fiducia e trasformato la crisi in un'opportunità di apprendimento.

CREARE UNA CULTURA ORGANIZZATIVA ORIENTATA AL PROBLEM-SOLVING

La risoluzione dei problemi non dovrebbe limitarsi alle situazioni di crisi. Una scuola resiliente promuove una cultura in cui le sfide sono viste come opportunità di crescita.

Azioni chiave per i dirigenti

- Dimostrare apertura: ammettere quando non si ha una soluzione immediata e mostrare come la si
sta cercando.
- Celebrare chi risolve i problemi: riconoscere il personale e gli studenti che dimostrano soluzioni creative alle difficoltà provenienti dal mondo digitale.
- Integrare le diverse materie: incoraggiare gli insegnanti a progettare lezioni che prevedano la valutazione di dilemmi e la proposta di soluzioni.
- Collegare l'educazione civica: qualificate la risoluzione dei problemi come parte della preparazione degli studenti a una partecipazione democratica e responsabile nella società.

AZIONI CHIAVE PER LA RISOLUZIONE DEI PROBLEMI



STRUMENTI PRATICI PER I DIRIGENTI

Problem-solving per dirigenti

- Quando affronto dilemmi digitali, applico procedure strutturate (ad esempio STOP). ☐
- Gli insegnanti della mia scuola sono formati su strategie coerenti di risoluzione dei problemi. ☐
- Gli studenti vengono introdotti a procedure decisionali per muoversi in contesti digitali. ☐
- Abbiamo protocolli chiari per rispondere alle crisi digitali. ☐
- I genitori sono coinvolti nella comunicazione durante le crisi come partner alla pari. ☐
- Riflettiamo sui problemi dopo la loro risoluzione per imparare dal passato e migliorare in futuro. ☐

Risorse consigliate

- Prospettive dell'OCSE sulle competenze: ricerca sulla risoluzione dei problemi nelle società digitali.[4]
- Common Sense Education: Programmi didattici sul processo decisionale digitale.[5]
- Strumenti del progetto SAILS: esercizi basati su scenari per la formazione in classe e del personale
- MindTools Problem-Solving Frameworks: strategie adattabili ai contesti di leadership.[6]

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

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

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

CONCLUSIONE

La risoluzione dei problemi nelle scuole non riguarda più solo la gestione quotidiana. In un mondo digitale, i dirigenti devono essere preparati a crisi improvvise legate alla disinformazione, guasti tecnici e conflitti online che possono avere un impatto sugli studenti, sul personale e sulla comunità in generale.

Una risoluzione efficace dei problemi comporta:

- Lo sviluppo di approcci critici, creativi e sicuri da parte dei dirigenti stessi.
- Fornire agli insegnanti strutture e protocolli condivisi.
- Integrare le capacità decisionali nella didattica.
- Rispondere alle crisi con calma, chiarezza e azioni costruttive.

Quando i dirigenti scolastici promuovono la risoluzione dei problemi come cultura organizzativa della scuola, preparano le loro comunità non solo a sopravvivere alle difficoltà provenienti dall'ambito digitale che pongono la scuola alla prova, ma anche a diventare più forti grazie ad esse.

CAPITOLO 5

PENSIERO CRITICO

PERCHÉ IL PENSIERO CRITICO È IMPORTANTE NELLE SCUOLE

Il pensiero critico è la capacità di mettere in discussione, analizzare e valutare le informazioni piuttosto che accettarle per buone. Nel mondo digitale, dove ogni studente, ogni insegnante è esposto quotidianamente a migliaia di post, immagini e video, questa abilità non è facoltativa, ma essenziale.

Per le scuole, il pensiero critico è più di una semplice competenza accademica. È alla base della resilienza digitale, della cittadinanza responsabile e del processo decisionale informato. Senza di esso:

- Gli studenti potrebbero accettare acriticamente teorie complottiste o contenuti online dannosi.
- Gli insegnanti potrebbero condividere informazioni non verificate con le classi, diffondendo involontariamente disinformazione.
- I genitori potrebbero perdere fiducia nelle scuole se i dirigenti non fossero in grado di dimostrare un impegno trasparente e critico nei confronti delle dicerie o delle politiche.

Per i dirigenti, la sfida è duplice: sviluppare le proprie capacità di pensiero critico come modelli di riferimento e creare una cultura scolastica in cui siano incoraggiati il dubbio e il ragionamento basato sulle prove.

SVILUPPARE LE CAPACITÀ DI PENSIERO CRITICO DEI DIRIGENTI

Prima di promuovere il pensiero critico tra il personale e gli studenti, i dirigenti devono rafforzare le proprie capacità. Un dirigente che reagisce in modo impulsivo alle dicerie che circolano online o prende decisioni basate su prove incomplete mina la cultura che sta cercando di costruire.

Domande chiave di riflessione per i dirigenti

1. Quando ricevo nuove informazioni, mi chiedo: chi le ha prodotte e perché?
2. Cerco più punti di vista prima di prendere decisioni?
3. Controllo se ci sono bias inconsci nelle mie supposizioni?
4. Dimostro trasparenza spiegando il mio ragionamento al personale e ai genitori?

Strategie pratiche per i leader

- Fermatevi prima di reagire: allenatevi a verificare prima di rispondere alle controversie online o ai reclami dei genitori.
- Utilizzate schemi critici: applicate procedure come le “5 W” (chi (who), cosa (what), quando (when), dove (where), perché (why)) quando esaminate le informazioni.
- Interagite con punti di vista contrastanti: leggete fonti diverse per evitare la formazione di camere d’eco, specialmente su questioni controverse.
- Condividete il vostro processo di pensiero: durante le riunioni, spiegate non solo la vostra decisione, ma anche come siete arrivati a essa, dando l’esempio di un approccio critico alle altre persone coinvolte.

Promuovere il pensiero critico in tutta la scuola

Una cultura del pensiero critico non può essere lasciata al caso, ma deve essere deliberatamente integrata.

Azioni della dirigenza

1. Integrazione nel programma scolastico: assicurarsi che il pensiero critico non sia limitato a una sola materia (come l’ICT o l’educazione civica), ma sia integrato nelle scienze, nella storia, nella letteratura e nelle arti.
2. Modelli di valutazione: premiare gli studenti che pongono domande e mettono in discussione le ipotesi, non solo quelli che danno la risposta “giusta”.

3. Collaborazione del personale: incoraggiare gli insegnanti a condividere il modo in cui integrano il pensiero critico nelle loro lezioni.

4. Ambiente sicuro: creare un clima in cui gli studenti si sentano a proprio agio nel porre domande difficili senza timore di essere ridicolizzati o puniti.

Se i programmi scolastici nazionali o i quadri di riferimento delle competenze descrivono il pensiero critico e l'alfabetizzazione mediatica, utilizzate tali riferimenti quando definite gli obiettivi della vostra scuola. Collegare la pratica didattica a queste aspettative politiche può anche rafforzare la vostra posizione quando richiedete formazione o risorse.

In linea con la scheda HEADstart n. 4, le attività di pensiero critico dovrebbero sempre basarsi su un quadro di valori chiaramente articolato che enfatizzi la dignità umana, l'equità e il dialogo rispettoso. Rendere visibili questi valori nelle azioni amministrative e gestionali e nei regolamenti aiuta gli studenti a comprendere perché determinati tipi di comportamenti e contenuti online sono eticamente inaccettabili.

Esempio: integrare il pensiero critico nella storia

Invece di limitarsi a memorizzare fatti storici, gli studenti sono incoraggiati a confrontare il modo in cui fonti diverse presentano lo stesso evento. I dirigenti hanno supportato gli insegnanti fornendo un kit di strumenti interdisciplinare sulla valutazione delle fonti. Ciò ha contribuito a qualificare il mettere in discussione come abilità preziosa, non come segno di sfida.

SOSTENERE GLI INSEGNANTI NELLO SVILUPPO DEL PENSIERO CRITICO

Gli insegnanti stessi devono avere fiducia nelle loro capacità critiche per sostenere efficacemente gli studenti. Molti si sentono sotto pressione per "coprire rapidamente i contenuti" e possono trascurare il tempo necessario per approfondire le domande. I dirigenti possono affrontare questo problema:

- Formazione professionale: fornire formazione sulle tecniche di messa in discussione e sull'analisi delle fonti digitali.
- Condivisione delle risorse: offrire modelli, liste per la verifica e attività didattiche incentrate sulla valutazione delle informazioni.
- Incoraggiamento: riconoscere e celebrare gli insegnanti che promuovono con successo discussioni critiche, anche quando il risultato è articolato piuttosto che chiaramente definito.
- Fungere da modelli: mostrare agli insegnanti che è accettabile non avere tutte le risposte: ciò che conta è la volontà di pensare in modo critico insieme agli studenti.

Esempio: apprendimento guidato da pari

In una scuola, gli insegnanti hanno creato un "circolo di pensiero critico" in cui il personale osservava le lezioni degli altri colleghi, concentrandosi in particolare sulle strategie di messa in discussione. Il dirigente ha sostenuto questa iniziativa assegnando tempo per le riunioni e riconoscendola nelle valutazioni professionali. Gli insegnanti hanno riferito che la loro sicurezza nel gestire le domande degli studenti è migliorata in modo significativo.

Sostenere gli studenti nell'approccio critico ai contenuti digitali

Gli studenti sono spesso consumatori accaniti di media digitali, ma meno abili nel valutarli. I dirigenti devono garantire che le aule diventino luoghi in cui agli studenti venga insegnato a rallentare, riflettere e porre domande.

Strategie per studenti

- Esercizi pratici: confrontate due notizie sullo stesso evento e discutete quale sia più credibile e perché.
- Domande guidate: insegnate agli studenti semplici domande come "Chi l'ha detto?" e "Quali prove lo dimostrano?".
- Gioco di ruolo: chiedete agli studenti di assumere il ruolo di "verificatori dei fatti" nei dibattiti in classe.
- Lavoro di progetto: assegnate progetti di ricerca che richiedono la valutazione delle fonti, non solo la raccolta di informazioni.

Esempio: club di fact-checking guidato da studenti

Una scuola secondaria ha creato un club studentesco in cui i partecipanti verificavano le notizie di dubbia affidabilità. Gli studenti hanno prodotto brevi relazioni. Con l'approvazione del dirigente, il club è diventato una voce autorevole tra gli studenti e ha contribuito a rendere comune l'approccio critico ai contenuti online.

QUANDO LE COSE VANNO MALE: DALLE SFIDE ALLE CRISI

Il pensiero critico è particolarmente prezioso nei momenti di confusione o tensione, quando la misinformazione le notizie non verificate si diffondono rapidamente. I dirigenti hanno bisogno di approcci chiari per mantenere la credibilità e prevenire il panico.

Scenari comuni

- Si diffonde la voce che un insegnante è stato licenziato per cattiva condotta.
- I genitori diffondono teorie complottiste su una nuova politica scolastica.
- Gli studenti diffondono immagini manipolate che suggeriscono incidenti pericolosi nella scuola.

Strategia di risposta del dirigente

1. Verificare: accertare rapidamente i fatti attraverso canali affidabili.
2. Riconoscere l'incertezza: se non si conosce ancora tutta la verità, dirlo onestamente
3. Comunicare in modo chiaro: fornire aggiornamenti in un linguaggio semplice, privo di gergo e di toni difensivi.
4. Educare attraverso la crisi: utilizzare l'incidente come lezione di pensiero critico nel mondo reale per il personale, gli studenti e i genitori.



CASO DI STUDIO: "L'IMMAGINE MANIPOLATA"

È apparsa online una foto che mostrava evidenti atti di vandalismo nella mensa scolastica, accompagnata da commenti che affermavano che gli studenti erano "fuori controllo". I genitori hanno iniziato a condividerla nei gruppi della comunità locale.

RISPOSTA DEL DIRIGENTE

- Il preside della scuola ha verificato le riprese delle telecamere a circuito chiuso, che hanno dimostrato che l'immagine era stata alterata digitalmente.
- È stata rilasciata una dichiarazione chiara ai genitori per spiegare la manipolazione e rassicurarli sul comportamento degli studenti.
- Durante le assemblee, l'episodio è stato utilizzato per insegnare agli studenti come modificare le immagini e l'importanza di mettere in discussione le immagini che si trovano online.

RISULTATO

Durante le assemblee, l'incidente è stato utilizzato per insegnare agli studenti l'editing delle immagini e l'importanza di mettere in discussione le immagini online.

CREARE UNA CULTURA DI ISTITUTO DEL PENSIERO CRITICO

Il pensiero critico non può essere imposto: deve essere incoraggiato attraverso la fiducia, l'apertura mentale e un rinforzo costante. I dirigenti svolgono un ruolo fondamentale nel radicarlo nell'etica dell'istituto.

Azioni chiave per i dirigenti

- Promuovere la curiosità: premiare gli studenti che fanno domande, non solo quelli che forniscono risposte.
- Incoraggiare la riflessione del personale: chiedere agli insegnanti di condividere il modo in cui modellano le domande durante le lezioni.
- Comunicare in modo trasparente: dimostrare il pensiero critico nelle comunicazioni della leadership, specialmente durante le crisi.
- Coinvolgere i genitori: offrire workshop alle famiglie sulla valutazione delle informazioni, assicurando che il pensiero critico si estenda oltre i confini della scuola.

STRUMENTI PRATICI PER I DIRIGENTI

Lista per la verifica del pensiero critico per dirigenti

- Nei miei comunicati do l'esempio ponendo domande critiche. ☐
- Gli insegnanti hanno accesso a formazione e risorse per promuovere il pensiero critico. ☐
- Agli studenti vengono insegnate in modo esplicito strategie di valutazione in tutte le materie. ☐
- La nostra scuola riconosce e premia la curiosità e la capacità di porre domande. ☐
- Utilizziamo gli episodi di disinformazione come opportunità di apprendimento. ☐
- I genitori sono coinvolti nelle iniziative di pensiero critico come risorse e partner alla pari. ☐

Risorse consigliate

- Programma di studi dell'UNESCO sull'alfabetizzazione mediatica e informativa[7]
- News Literacy Project (Stati Uniti) – risorse pronte per l'uso in classe[8]
- Full Fact (Regno Unito) – strumenti per verificare le affermazioni[9]
- Esercizi del progetto SAILS – scenari pratici di pensiero critico per le scuole[10]

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

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

9 https://fullfact.org/

10 https://sails.deusto.es/

CONCLUSIONE

Il pensiero critico è la pietra angolare dell'alfabetizzazione digitale. Per i dirigenti, è sia un'abilità personale da praticare sia un valore culturale da integrare.

- Rafforzando le proprie capacità di porre domande.
- Supportando gli insegnanti con formazione e strumenti.
- Fornendo agli studenti semplici strategie di valutazione.
- Comunicando in modo trasparente con i genitori e le comunità.

I dirigenti possono trasformare le scuole in spazi in cui vengono valorizzate la verità, la curiosità e le prove concrete.

In un'epoca di disinformazione, una scuola che promuove il pensiero critico non si limita a insegnare agli studenti come avere successo a livello accademico. Li prepara a prosperare come cittadini riflessivi e responsabili in un mondo in cui le informazioni sono abbondanti, ma la verità deve essere ricercata attivamente.

STRATEGIA DI RISPOSTA DEI DIRIGENTI AI PROBLEMI DEL PENSIERO CRITICO



CAPITOLO 6

BULLISMO E CYBERBULLISMO

PERCHÉ IL BULLISMO MERITA L'ATTENZIONE DEI DIRIGENTI

Il bullismo non è una novità, ma le tecnologie digitali ne hanno amplificato la portata e l'impatto. Un commento crudele che un tempo rimaneva confinato al cortile della scuola ora può essere condiviso con centinaia di persone in pochi secondi. Foto o video possono essere alterati e diffusi su larga scala, rendendo l'umiliazione pubblica e duratura. Per le scuole, il bullismo, in particolare il cyberbullismo, è una delle sfide più urgenti per la sicurezza e il benessere degli studenti.

La ricerca DRONE evidenzia una realtà critica ma spesso trascurata: sebbene il bullismo tra pari sia la forma più visibile, gli studenti a volte sono vittime di bullismo da parte di insegnanti o familiari e viceversa. Queste forme di abuso sono spesso nascoste, sottovalutate e profondamente dannose. I dirigenti devono i riconoscerle, creare sistemi di segnalazione sicuri e agire con decisione.

Comprendere il bullismo e il cyberbullismo

Il bullismo è un comportamento ripetuto e intenzionale che causa danni, squilibrio di potere e sofferenza. Il cyberbullismo si riferisce al bullismo che avviene attraverso piattaforme digitali, tra cui:

- Messaggi, meme o post offensivi.
- Account falsi che impersonano uno studente.
- Esclusione da gruppi online.
- Diffusione di notizie non verificate o immagini in formato digitale.

Caratteristiche principali del cyberbullismo

- Raggiungibilità 24 ore su 24, 7 giorni su 7: le vittime possono sentirsi senza via di scampo.
- Amplificazione: i contenuti online possono diffondersi rapidamente e su larga scala.
- Anonimato: i bulli possono nascondersi dietro profili falsi.
- Persistenza: i contenuti dannosi possono rimanere accessibili a tempo indeterminato.

Bullismo da parte di insegnanti: il problema "nascosto"

È spiacevole ma necessario riconoscere che alcuni studenti sono vittime di bullismo da parte di coloro che dovrebbero prendersi cura di loro. Il bullismo online (ma anche offline) da parte di insegnanti può includere:

- Umiliare o ridicolizzare pubblicamente uno studente.
- Prendere di mira ingiustamente uno studente con misure disciplinari severe.
- Fare commenti discriminatori o umilianti.
- Usare il sarcasmo o l'autorità per intimidire piuttosto che per guidare.

Perché spesso non viene notato

- Gli studenti potrebbero temere ritorsioni o credere che nessuno li ascolterà.
- I colleghi potrebbero qualificare comportamenti severi come "metodi didattici rigorosi".
- I genitori potrebbero esitare a mettere in discussione le figure autoritarie.

Responsabilità della dirigenza

- Stabilire una politica di tolleranza zero: il bullismo è inaccettabile indipendentemente da chi lo perpetra.
- Fornire sistemi di segnalazione riservati per studenti e genitori.
- Garantire indagini indipendenti sulle accuse che coinvolgono il personale.
- Promuovere una cultura in cui i rapporti rispettosi e di sostegno tra insegnanti e studenti siano la norma.

Garantire che le procedure anti-bullismo e anti-cyberbullismo rispecchino le definizioni, le modalità di segnalazione e le soglie stabilite nelle normative nazionali in materia di tutela e protezione dei minori. Fare riferimento a queste politiche nei documenti scolastici aiuta il personale a riconoscere quando un incidente deve essere segnalato al di fuori della scuola.

In seguito all'HEADstart n. 11, il codice di condotta della scuola dovrebbe indicare esplicitamente che le aspettative legali ed etiche in materia di rispetto, non discriminazione e privacy si applicano a tutte le interazioni digitali. Dovrebbe chiarire quali comportamenti possono costituire molestie, incitamento all'odio o condivisione illegale di immagini o dati personali e come questi saranno registrati e segnalati.

Bullismo da parte dei membri della famiglia

Sebbene le scuole non possano controllare l'ambiente familiare, devono riconoscere quando gli studenti subiscono bullismo da parte dei genitori, dei fratelli, o di altre persone che si prendono cura di loro.
Il bullismo familiare può includere:

- Critiche costanti o svalutazione dei ragazzi.
- Sorveglianza digitale o umiliazione tramite i social media.
- Molestie tra fratelli tollerate o incoraggiate dai genitori.

Segnali che insegnanti e dirigenti potrebbero notare

- Uno studente è costantemente ansioso o introverso dopo il fine settimana.
- Improvvisa riluttanza a utilizzare dispositivi digitali.
- Prove che i membri della famiglia condividono contenuti imbarazzanti online.

Ruolo della dirigenza

- Formare il personale a riconoscere i segnali di allarme.
- Fornire agli studenti modi sicuri e riservati per rivelare le loro preoccupazioni.
- Collaborare con i servizi di tutela per sostenere il bambino e, se necessario, intervenire.

Il bullismo tra pari è ancora una preoccupazione

Sebbene meno frequente di quanto talvolta suggeriscano le narrazioni pubbliche, il bullismo tra pari rimane comunque dannoso. Può minare l'autostima, il rendimento scolastico e il senso di appartenenza. I dirigenti dovrebbero trattare con serietà anche i piccoli incidenti per evitare che la situazione degeneri.

Tipi di cyberbullismo tra pari

- Esclusione di gruppo da chat o giochi.
- "Attacchi di gruppo" in cui più studenti prendono di mira un compagno o una compagna
- Condivisione di immagini o video imbarazzanti senza consenso.

SOSTENERE GLI INSEGNANTI NELLA GESTIONE DEL BULLISMO

Nella maggior parte dei casi, il cyberbullismo non avviene a scuola, ma i suoi effetti possono essere avvertiti a scuola. Se ciò accade, gli insegnanti e i dirigenti potrebbero dover collaborare con i genitori e gli studenti per affrontarlo.

Gli insegnanti sono spesso i primi a venire a conoscenza dei casi di bullismo, ma possono sentirsi impreparati ad agire, soprattutto se sono coinvolte prove digitali. I dirigenti possono responsabilizzare gli insegnanti:

- Fornendo procedure chiare: gli insegnanti devono sapere esattamente come segnalare e notificare gli incidenti.
- Formazione sulle prove digitali: gli insegnanti devono capire come conservare correttamente screenshot, messaggi o post.
- Incoraggiando approcci basati sull'empatia: gli insegnanti dovrebbero rivolgersi sia alle vittime che ai responsabili, concentrandosi sulla riparazione del danno e non solo sulla punizione.
- Sostenendoli: gli insegnanti devono sentire che la dirigenza li sosterrà se intervengono, anche in casi delicati che coinvolgono genitori o personale.

SOSTENERE GLI STUDENTI CHE SUBISCONO IL BULLISMO

I dirigenti devono garantire che gli studenti che subiscono il bullismo, sia da parte di compagni, insegnanti e familiari, ricevano un sostegno immediato e a lungo termine. È inoltre importante ricordare che il bullismo è un comportamento appreso, quindi la maggior parte dei perpetratori sono anche vittime o sono stati esposti al bullismo come spettatori. Pertanto, anche i bulli devono essere trattati con attenzione e l'azione della dirigenza dovrebbe mirare a individuare le cause del bullismo.

Azioni chiave

- Segnalazione sicura: diverse opzioni di segnalazione (moduli digitali, personale di fiducia, mentori tra i coetanei).
- Azione rapida: indagini e comunicazioni tempestive per dimostrare la serietà dell'impegno.
- Consulenza e sostegno: accesso all'assistenza pastorale, al mentoring o a servizi esterni.
- Pratiche riparative: ove possibile, opportunità sicure per risolvere i problemi e ricostruire la fiducia.

QUANDO LE COSE VANNO MALE: DALLE DIFFICOLTÀ ALLE CRISI

Gli episodi di bullismo possono degenerare in crisi che coinvolgono l'intera comunità scolastica.

Crisi comuni

- Un video di un episodio di bullismo diventa virale, attirando l'attenzione dei media.
- Un insegnante viene accusato di aver umiliato gli studenti online.
- I genitori utilizzano i social media per attaccare il personale scolastico per la sua presunta inazione.

Struttura della dirigenza in caso di crisi

1. Risposta immediata: fermare il danno, rimuovere i contenuti dannosi e garantire la sicurezza degli studenti.

2. Comunicazione trasparente: condividere aggiornamenti verificati con genitori, personale, studenti.

3. Protezione della privacy: evitare di rendere pubblici i nomi delle vittime o dei responsabili.

4. Imparare e prevenire: dopo la risoluzione, rivedere le politiche e garantire che le lezioni siano condivise in tutta la scuola.

QUADRO DI RIFERIMENTO PER LA GESTIONE DELLE CRISI IN CASO DI BULLISMO O CYBERBULLISMO





CASO DI STUDIO 1: BULLISMO DA PARTE DI UN INSEGNANTE

Uno studente dell'ottavo anno ha riferito che un insegnante prendeva regolarmente in giro il suo accento davanti ai compagni. Inizialmente, la direzione ha esitato ad agire, preoccupata per il danno alla reputazione. Alla fine, altri studenti hanno confermato il comportamento.

Risposta:

- È stato nominato un investigatore esterno.
- L'insegnante è stato sospeso durante le indagini.
- È stata organizzata una formazione per tutto il personale sui pregiudizi inconsci e sulla comunicazione rispettosa.

Risultato:

Il caso era difficile ma essenziale. Agendo con decisione, la scuola ha rafforzato il proprio impegno a favore della dignità degli studenti e ha messo in atto misure di tutela più efficaci.

CASO DI STUDIO 2: VIDEO VIRALE SUL BULLISMO TRA PARI

In una scuola secondaria, una rissa avvenuta nel cortile è stata filmata e diffusa ampiamente online, con una didascalia volta a umiliare uno studente.

Risposta:

- La direzione ha collaborato con le piattaforme dei social media per rimuovere il video.
- Sono stati contattati i genitori di tutti gli studenti coinvolti.
- Durante le assemblee sono stati affrontati i temi della cittadinanza digitale e della responsabilità dei testimoni.
- Allo studente preso di mira è stata offerta assistenza psicologica.

Risultato:

La scuola ha utilizzato l'incidente come momento di apprendimento, rafforzando una cultura dell'attenzione e della responsabilità digitale.

CREARE UNA CULTURA SCOLASTICA RESISTENTE AL BULLISMO

La prevenzione è più efficace della gestione delle crisi. I dirigenti dovrebbero creare un clima scolastico in cui qualsiasi forma di bullismo sia inaccettabile.

Passaggi chiave

- Chiarezza delle politiche: garantire che le politiche contro il bullismo includano esplicitamente gli insegnanti e il contesto familiare.
- Formazione regolare: aggiornare annualmente tutto il personale sul riconoscimento e la gestione del bullismo.
- Voce degli studenti: coinvolgere gli studenti nella definizione delle strategie anti-bullismo.
- Collaborazione con i genitori: offrire ai genitori workshop collaborativi con gli insegnanti sulla responsabilità digitale e le dinamiche familiari.
- Visibilità dei valori: promuovere il rispetto, l'empatia e l'inclusione nelle comunicazioni e negli eventi scolastici.

STRUMENTI PRATICI PER I DIRIGENTI

Lista di controllo sul bullismo per i dirigenti

- Le politiche riguardano il bullismo nei confronti degli insegnanti e delle famiglie, non solo gli episodi tra pari. ☐
- Il personale riceve una formazione annuale sul riconoscimento e la segnalazione dei casi di bullismo. ☐
- Glli studenti dispongono di canali di segnalazione sicuri e accessibili. ☐
- Sono in vigore protocolli per la raccolta di prove digitali. ☐
- Le risposte danno priorità alla sicurezza, alla dignità e alle pratiche riparative. ☐
- I genitori sono coinvolti nella prevenzione e nella risposta come partner alla pari. ☐

Risorse consigliate

- Anti-Bullying Alliance (UK) – formazione e strumenti per le scuole.[11]
- UNICEF Guidance – bullismo e sicurezza online.[12]
- Ditch the Label – risorse sul bullismo tra pari e sul bullismo digitale.[13]
- SAILS Project Tools – checklist per riconoscere i comportamenti di bullismo. (https://library.parenthelp.eu/seafarers-guide/, https://library.parenthelp.eu/captains-handbook-sails-resource-for-school-leaders/)

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

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

13 https://ditchthelabel.org/

CONCLUSIONE

Il bullismo, sia esso perpetrato da coetanei, insegnanti o familiari, è una grave violazione della fiducia e della sicurezza. I dirigenti devono:

- Affrontare realtà scomode, compreso il bullismo da parte degli adulti nei confronti dei bambini.
- Fornire agli insegnanti formazione e supporto per agire con sicurezza.
- Garantire che gli studenti si sentano ascoltati, protetti e sostenuti.
- Rispondere alle crisi con chiarezza, compassione e azioni decisive.

Creando una cultura in cui il rispetto è imprescindibile e il bullismo non è mai tollerato, i dirigenti scolastici possono trasformare le scuole in luoghi sicuri e dignitosi. In questo modo, non solo proteggono i singoli studenti, ma rafforzano anche l'intera comunità.

CAPITOLO 7

CYBERSECURITY

PERCHÉ LA CYBERSECURITY È UN PROBLEMA DI LEADERSHIP

La sicurezza informatica nelle scuole non è solo una questione tecnica che riguarda il personale IT. È una responsabilità strategica della leadership. Una singola violazione, che si tratti di un account di posta elettronica hackerato, di una password rubata o di dati degli studenti trapelati, può minare la fiducia dei genitori, danneggiare

il morale del personale e persino mettere a rischio l'incolumità fisica dei bambini.

L'infrastruttura digitale è ormai essenziale quanto l'acqua e l'elettricità. I dirigenti scolastici devono trattare la sicurezza informatica con la stessa serietà, garantendo che i sistemi siano protetti, il personale sia formato e gli studenti siano al sicuro.

La ricerca DRONE mostra che molti dirigenti sottovalutano la sicurezza informatica fino a quando non si verifica una crisi. Troppo spesso la sicurezza è vista come una "questione secondaria", quando in realtà richiede politiche, cultura e vigilanza a livello scolastico.

La sicurezza informatica in ambito scolastico

Le scuole sono obiettivi attraenti per gli attacchi informatici perché detengono dati sensibili:

- Documenti personali degli studenti, comprese informazioni sulla salute e sulla sicurezza.
- Dettagli relativi all'assunzione del personale e alle buste paga.
- Risultati degli esami e dati di valutazione.
- Credenziali di accesso per diversi sistemi di apprendimento online.

Le minacce più comuni includono:

- E-mail di phishing che inducono il personale a rivelare le password.
- Attacchi ransomware che bloccano i file fino al pagamento di un riscatto.
- Violazioni dei dati che espongono le informazioni degli studenti e del personale.
- Dispositivi non sicuri che si connettono alle reti scolastiche senza protezioni.

SVILUPPARE LE COMPETENZE DEI LEADER IN MATERIA DI CYBERSECURITY

Prima di proteggere gli altri, i leader devono sviluppare le proprie competenze in materia di sicurezza digitale. Se i leader stessi cadono vittime di truffe di phishing o utilizzano password deboli, non possono promuovere in modo credibile una cultura della sicurezza informatica.

Domande di autovalutazione

1. Utilizzo password complesse e uniche (o un gestore di password) per gli account scolastici?
2. Sono sicuro di saper identificare e-mail o link sospetti?
3. Mantengo aggiornati i miei dispositivi con le ultime versioni di software e patch di sicurezza?
4. Sono a conoscenza del piano di risposta agli incidenti della scuola in caso di violazioni dei dati?
5. Adotto pratiche sicure quando condivido informazioni con i genitori e il personale?

Se la risposta a una di queste domande è “no”, il dirigente deve dare priorità alla formazione personale in materia di sicurezza informatica.

SUPPORTARE GLI INSEGNANTI NELLA CONSAPEVOLEZZA DELLA CYBERSECURITY

Gli insegnanti spesso gestiscono informazioni sensibili: voti, relazioni sulla sicurezza, comunicazioni personali con i genitori. Senza una formazione adeguata, potrebbero inavvertitamente divulgare dati o cadere vittime di truffe.

Azioni della dirigenza

- Formazione obbligatoria: organizzare sessioni annuali sulla consapevolezza del phishing, l'igiene delle password e la protezione dei dati.
- Simulazioni pratiche: utilizzare e-mail di phishing simulate per testare la consapevolezza e incoraggiare la discussione.
- Protocolli chiari: gli insegnanti devono sapere esattamente come segnalare e-mail sospette o potenziali violazioni.
- Sostegno, non biasimo: inquadrare la formazione come empowerment, non come punizione: gli errori dovrebbero diventare opportunità di apprendimento.

Allineare le regole di sicurezza informatica della scuola alla legislazione nazionale o regionale in materia di protezione dei dati e agli standard di sicurezza del settore educativo. Indicare chiaramente questi riferimenti nei manuali del personale ricorda a tutti che la sicurezza digitale è sia un obbligo legale che una priorità pedagogica.

HEADstart #20 ricorda ai dirigenti che la sicurezza informatica è indissociabile dalla conformità legale al GDPR e dai diritti dei minori in materia di protezione dei dati. I dirigenti dovrebbero quindi conoscere il proprio responsabile della protezione dei dati, comprendere gli obblighi di segnalazione nazionali e garantire che ogni misura tecnica sia supportata da pratiche di trattamento dei dati legali e trasparenti.

SOSTENERE GLI STUDENTI NELLA CYBERSECURITY

Anche gli studenti hanno bisogno di una guida per proteggersi online. Sebbene le lezioni di informatica possano coprire alcune nozioni di base, i dirigenti dovrebbero garantire che la sicurezza informatica sia integrata in iniziative più ampie di alfabetizzazione digitale.

Strategie per gli studenti

- Pratiche relative alle password: insegnare agli studenti a creare passphrase forti e facili da ricordare.
- Consapevolezza della privacy: incoraggiarli a riflettere criticamente prima di condividere dati personali online.
- Sicurezza dei dispositivi: promuovere un uso sicuro dei dispositivi scolastici e personali (aggiornamenti, accessi sicuri).
- Apprendimento tra pari: creare opportunità per gli studenti più grandi di fare da mentori ai compagni più giovani in materia di sicurezza informatica.

QUANDO LE COSE VANNO MALE – DALLE SFIDE ALLE CRISI

Nonostante le precauzioni, le scuole possono trovarsi ad affrontare incidenti di sicurezza informatica.

Crisi comuni

- Un attacco ransomware crittografa i file della scuola, richiedendo un pagamento.
- Un membro del personale clicca su un'e-mail di phishing, esponendo le credenziali di accesso.
- Un'e-mail inviata da un gruppo di genitori divulga informazioni personali sugli studenti.
- Un account social media hackerato diffonde messaggi falsi a nome della scuola.

Struttura di gestione delle crisi per i dirigenti

1. Contenere l'incidente: scollegare immediatamente i sistemi compromessi.
2. Informare le persone chiave: avvisare il personale IT, le autorità competenti e i responsabili della protezione dei dati.
3. Comunicare con cautela: condividere aggiornamenti chiari e basati sui fatti con il personale e i genitori. Evitare speculazioni.
4. Supportare le persone coinvolte: in caso di fuga di dati, fornire indicazioni sul monitoraggio e sulla protezione.
5. Imparare e migliorare: riesaminare l'incidente per rafforzare le politiche e la formazione.



CASO DI STUDIO 1: L'E-MAIL DI PHISHING

Il responsabile amministrativo di una scuola secondaria ha ricevuto un'e-mail che sembrava provenire dal dirigente scolastico e chiedeva un trasferimento urgente di fondi per "attrezzature". Il responsabile era quasi sul punto di effettuare il trasferimento, ma si è fermato per verificare direttamente con il dirigente, evitando una perdita di denaro.

Lezioni di leadership:

- La formazione regolare aveva aumentato la consapevolezza, permettendo al responsabile di fermarsi e verificare
- La cultura della comunicazione aperta ha incoraggiato la verifica piuttosto che l'adesione cieca.
- Dopo l'incidente, la scuola ha aggiornato le proprie procedure finanziarie richiedendo l'autorizzazione di più persone.

CASO DI STUDIO 2: L'ATTACCO RANSOMWARE

I sistemi di una scuola elementare sono stati bloccati da un ransomware, rendendo inaccessibili i sistemi di registrazione delle presenze, di valutazione e di comunicazione. Gli hacker hanno chiesto un riscatto.

Risposta:

- La scuola ha contattato immediatamente le autorità locali e gli specialisti IT.
- I backup sono stati ripristinati, evitando il pagamento del riscatto.
- I genitori sono stati informati tramite lettere cartacee e bacheche comunitarie.
- È stata introdotta una formazione sul ransomware per tutto il personale.

Risultato:

La crisi ha evidenziato l'importanza dei backup offline e di una comunicazione trasparente. La fiducia dei genitori è aumentata grazie alla leadership onesta.

COSTRUIRE UNA CULTURA DELLA SICUREZZA INFORMATICA

La sicurezza informatica deve essere più di un insieme di regole: deve diventare una cultura condivisa in tutta la scuola.

Passi per i dirigenti

- Creare un clima di consapevolezza: parlare regolarmente di sicurezza informatica durante le riunioni del personale e nelle newsletter.
- Premiare la vigilanza: riconoscere il merito al personale o agli studenti che segnalano attività sospette.
- Normalizzare la cautela: incoraggiare un approccio del tipo “meglio prevenire che curare” nei confronti di link o allegati sconosciuti.
- Collaborare con i genitori: organizzare seminari per insegnanti e genitori sulla sicurezza informatica a casa, garantendo coerenza tra l’ambiente scolastico e quello familiare.



STRUMENTI PRATICI PER I DIRIGENTI

Lista di controllo sulla sicurezza informatica per i dirigenti

- Utilizzo password complesse e uniche e incoraggio il personale a fare lo stesso. ☐
- Il personale riceve una formazione annuale sulla sicurezza informatica con simulazioni. ☐
- Abbiamo un piano di risposta agli incidenti chiaro e collaudato. ☐
- I dati sensibili sono crittografati e sottoposti a backup regolari. ☐
- Agli studenti vengono insegnate pratiche di sicurezza informatica adeguate alla loro età ☐
- I genitori sono coinvolti nella sensibilizzazione alla sicurezza informatica a casa. ☐
- I rapporti con i fornitori di tecnologia includono chiare aspettative in materia di sicurezza. ☐

Risorse consigliate

- National Cybersecurity Centre (NCSC, Regno Unito) – linee guida per le scuole.[14]
- Progetto EU Kids Online – ricerca e risorse sulla sicurezza digitale dei bambini.[15]
- Common Sense Education – risorse didattiche sulla sicurezza informatica degli studenti.[16]
- Strumenti del progetto SAILS – liste di controllo ed esercizi pratici. (https://library.parenthelp.eu/captains-handbook-sails-resource-for-school-leaders/)

Basandosi sui documenti HEADstarts n. 20 e n. 21, la checklist sulla sicurezza informatica dovrebbe verificare se tutti i flussi di dati, gli strumenti di terze parti e le ubicazioni di archiviazione siano stati mappati e valutati in base ai principi del GDPR e della Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza (UNCRC). Dovrebbe inoltre verificare che le procedure di consenso, la minimizzazione dei dati, le regole di conservazione e i diritti di accesso o cancellazione degli alunni siano chiaramente definiti e comunicati.

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

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

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

CONCLUSIONE

La sicurezza informatica non è facoltativa, né è un gergo tecnico: si tratta di salvaguardare la fiducia, la sicurezza e l'integrità dell'intera comunità scolastica.

Per i dirigenti, una sicurezza informatica efficace significa:

- Rafforzare le proprie pratiche di sicurezza digitale.
- Garantire che il personale sia sicuro e supportato.
- Integrare la sicurezza informatica nell'apprendimento degli studenti.
- Rispondere in modo rapido e trasparente quando si verificano incidenti.

Una scuola sicura è quella in cui i dati degli studenti, il lavoro degli insegnanti e la fiducia della comunità sono tutti protetti. I dirigenti che considerano la sicurezza informatica una priorità culturale, e non solo una questione informatica, rafforzeranno la resilienza alle minacce e prepareranno gli studenti per un futuro digitale sicuro.

CAPITOLO 8

COSTRUIRE ALLEANZE

PERCHÉ È IMPORTANTE COSTRUIRE ALLEANZE

Le scuole non esistono in modo isolato. Interagiscono quotidianamente con fornitori di tecnologia, piattaforme di social media, agenzie governative, genitori, organizzazioni comunitarie e partner industriali. Queste relazioni possono fornire risorse preziose, strumenti innovativi e nuove opportunità per gli studenti. Ma possono anche esporre le scuole a contratti squilibrati, sfruttamento dei dati e dilemmi etici.

La ricerca DRONE evidenzia che i dirigenti scolastici spesso stringono partnership senza comprenderne appieno le conseguenze a lungo termine. Le decisioni relative alle licenze software, agli accordi di condivisione dei dati o alle sponsorizzazioni aziendali possono influenzare il modo in cui gli studenti apprendono, il modo in cui il personale lavora e il modo in cui viene mantenuta la fiducia delle famiglie.

I dirigenti scolastici devono quindi diventare dei gatekeeper critici: accogliendo le alleanze positive, rifiutando quelle di sfruttamento e assicurandosi che ogni relazione sostenga la missione della scuola di salvaguardare ed educare i giovani.

Valutare le relazioni digitali con aziende ed enti

Ogni contratto, sia esso stipulato con un grande fornitore di tecnologia o con una piccola start-up nel settore dell'istruzione, comporta dei rischi.

Domande chiave per i dirigenti prima di firmare qualsiasi accordo

1. Quali dati saranno raccolti? Informazioni personali su studenti e personale, dati comportamentali o modelli di utilizzo?
2. Chi è il proprietario dei dati? La scuola ne manterrà la proprietà o l'azienda potrà utilizzarli per scopi commerciali?
3. Quanto è trasparente l'azienda? Fornisce spiegazioni chiare e in linguaggio semplice dei termini?
4. Cosa succede alla scadenza del contratto? I dati saranno cancellati, trasferiti o venduti?
5. La partnership è in linea con i valori della scuola? Promuove l'equità, la sicurezza e l'apprendimento o serve principalmente gli interessi aziendali?

Misure pratiche

- Coinvolgere sia i consulenti legali che il personale addetto alla tutela prima della firma.

- Cercare recensioni indipendenti del prodotto o del servizio.
- Testare i nuovi strumenti su piccola scala prima di introdurli in tutta la scuola.
- Coinvolgere i genitori nelle discussioni sull'uso dei dati e sulle nuove piattaforme.

Quando valutate contratti o partnership, verificate che siano conformi alle normative nazionali in materia di protezione dei dati, appalti pubblici e attività commerciali nelle scuole. Indicare questi riferimenti normativi nella documentazione relativa alla partnership rafforza la vostra posizione nel caso in cui sia necessario rinegoziare o rescindere un accordo.

PROMUOVERE RELAZIONI DIGITALI ETICHE

Costruire alleanze non significa solo proteggere la scuola dai danni. Se gestite bene, le partnership possono arricchire l'apprendimento e creare opportunità significative.

Esempi di alleanze positive

- Collaborazioni con le università per la ricerca sull'alfabetizzazione digitale.
- Partnership con aziende locali che offrono tirocini online sicuri.
- Collaborazione con organizzazioni no profit per la formazione degli studenti alla resilienza.
- Progetti guidati dalla comunità sulla consapevolezza della sicurezza informatica.

Ruolo di leadership

- Stabilire uno standard etico: chiarire che la scuola non comprometterà la privacy degli studenti per ottenere un guadagno economico.
- Essere trasparenti: condividere apertamente contratti, accordi e decisioni con il personale e i genitori.
- Dare priorità all'equità: garantire che gli strumenti digitali siano accessibili a tutti gli studenti, non solo a quelli che dispongono di risorse a casa.

QUANDO LE COSE VANNO MALE: DALLE SFIDE ALLE CRISI

Anche le collaborazioni ben intenzionate possono andare male. I dirigenti devono essere pronti a reagire quando le alleanze minacciano i valori della scuola o la sicurezza degli studenti.

Scenari comuni

- Una società utilizza i dati degli studenti per scopi pubblicitari senza il loro consenso.
- Uno sponsor fa pressione sulla scuola affinché promuova i suoi prodotti in cambio di finanziamenti.

• I genitori scoprono che l'attività online dei propri figli su una piattaforma scolastica è stata tracciata per scopi commerciali.

Approccio alla leadership in situazioni di crisi

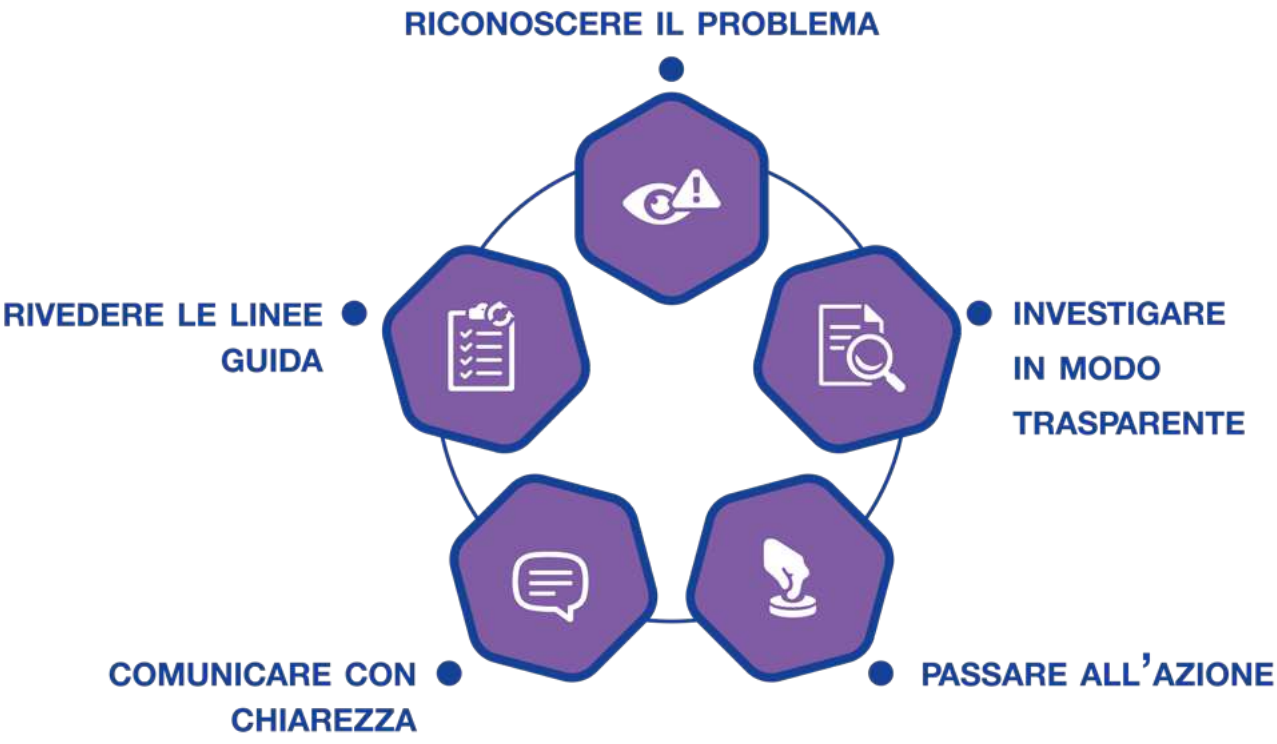
1. Riconoscere rapidamente il problema: non ritardare il riconoscimento delle preoccupazioni.

2. Indagare in modo trasparente: raccogliere i fatti e consultare i responsabili della protezione dei dati.

3. Agire con decisione: sospendere o interrompere la collaborazione se la fiducia è compromessa.

4. Comunicare in modo chiaro: informare i genitori, il personale e gli studenti su ciò che è accaduto, sulle misure adottate e sulle modalità di protezione.

5. Rivedere la politica: aggiornare le procedure di verifica dei contratti per evitare il ripetersi dei problemi.





CASO DI STUDIO 1: L'APP GRATUITA CON COSTI NASCOSTI

Una scuola ha adottato un'app gratuita di "aiuto allo studio" promossa come supporto per i compiti a casa. Alcuni mesi dopo, i genitori hanno notato che i bambini ricevevano pubblicità mirate basate sull'utilizzo dell'app. Da un'indagine è emerso che l'app vendeva i dati comportamentali degli studenti.

Risposta della dirigenza:

- Il contratto è stato immediatamente risolto.
- I genitori sono stati informati con una spiegazione chiara.
- È stata introdotta una formazione sul riconoscimento dei costi nascosti negli strumenti digitali "gratuiti".

Lezione: i prodotti digitali gratuiti spesso monetizzano i dati. I dirigenti devono garantire la trasparenza prima dell'adozione.

CASO DI STUDIO 2: LA PRESSIONE DELLA SPONSORIZZAZIONE

Un'azienda locale ha offerto una donazione consistente a una scuola in cambio dei diritti di denominazione di un premio studentesco. Il premio, tuttavia, era legato a una linea di prodotti commercializzati direttamente ai bambini.

Risposta della dirigenza:

- Il preside ha rifiutato l'offerta, spiegando il conflitto di interessi.
- Il rifiuto è stato comunicato pubblicamente per rafforzare gli standard etici.
- La scuola ha cercato fonti di finanziamento alternative nella comunità.

Lezione: Non tutti i soldi sono buoni soldi. L'allineamento etico deve guidare le decisioni di partnership.

ALLEANZE DELLA SCUOLA

Costruire alleanze con i genitori e le comunità

Le collaborazioni non si limitano alle aziende: i genitori e le comunità sono alleati fondamentali nella promozione dell'alfabetizzazione digitale e della resilienza.

Strategia per i dirigenti

- Workshop per i genitori: offrire formazione su disinformazione, sicurezza informatica e uso responsabile della tecnologia.
- Forum comunitari: creare spazi aperti in cui genitori e studenti possano sollevare preoccupazioni riguardo all'uso della tecnologia a scuola.
- Responsabilità condivisa: incoraggiare le famiglie a rafforzare le stesse lezioni di alfabetizzazione digitale a casa.

Quando i genitori sono coinvolti, la fiducia cresce e gli studenti ricevono una guida coerente sia a scuola che a casa.

Costruire alleanze con insegnanti e personale scolastico

Gli insegnanti sono in prima linea nell'attuazione delle iniziative digitali. Se si sentono esclusi dal processo decisionale, le partnership potrebbero fallire.

Azioni di leadership

- Coinvolgere i docenti nella valutazione dei nuovi strumenti e dei contratti.
- Garantire al personale il tempo e la formazione necessari per adattarsi.
- Ascoltare il feedback dei docenti sull'esperienza degli studenti con le piattaforme digitali.

Trattando gli insegnanti come co-creatori, i leader garantiscono che le alleanze rispondano alle realtà della classe, non solo agli obiettivi amministrativi.

Costruire alleanze con gli studenti

Gli studenti non sono consumatori passivi di tecnologia. Possono essere partner attivi nella creazione di ambienti digitali.

Idee pratiche

- Consigli digitali degli studenti: coinvolgere gli studenti nella revisione degli strumenti e delle linee guida per il digitale.
- Workshop condotti dai pari: formare gli studenti più grandi affinché fungano da mentori per i compagni in materia di sicurezza online.
- Feedback: sondare regolarmente gli studenti sulle loro esperienze di apprendimento digitale.

Queste alleanze responsabilizzano gli studenti e promuovono la cittadinanza digitale.

Creare un quadro di riferimento per alleanze etiche

Per sistematizzare le decisioni, i leader possono adottare un semplice quadro di riferimento per le partnership etiche:

1. Scopo: questa alleanza sostiene chiaramente gli obiettivi educativi?
2. Protezione: i diritti degli studenti e del personale sono tutelati?
3. Trasparenza: i termini e l'utilizzo dei dati vengono comunicati apertamente?
4. Equità: tutti gli studenti trarranno equamente beneficio da questa partnership?
5. Strategia di uscita: la scuola può recedere in modo sicuro, se necessario?

STRUMENTI PRATICI PER I DIRIGENTI

Checklist per la valutazione dell'alleanza

- Il contratto specifica chiaramente la proprietà dei dati? ☐
- I genitori sono informati delle nuove partnership digitali? ☐
- Esiste una strategia di uscita senza penali? ☐
- La partnership è in linea con i valori della scuola e gli standard di tutela dei minori? ☐
- Gli insegnanti e gli studenti sono coinvolti nel processo di valutazione? ☐
- L'accordo è stato esaminato da esperti legali o in materia di tutela? ☐

Risorse consigliate

- Linee guida del Consiglio d'Europa per partnership eque tra scuole e aziende.[17]
- Linee guida del Comitato europeo per la protezione dei dati – protezione dei dati nelle scuole.[18]
- Linee guida dell'UNICEF sui partenariati digitali – quadri etici per la collaborazione con i fornitori di tecnologia.[19]
- EdTech Evidence Exchange – recensioni indipendenti delle tecnologie didattiche.[20]
- Strumenti del progetto SAILS – liste di controllo per la valutazione di alleanze e contratti.[21]

17 https://rm.coe.int/prems-049222-gbr-2508-ligne-directrice-etablissements-a4-web-1-/1680a94c1b
18 https://www.edpb.europa.eu/our-work-tools/our-documents/topic/children_en
19 https://www.unicef.org/esa/media/3141/file/PolicyLab-Guide-DigitalConnectivity-Nov.6.18-lowres.pdf
20 https://www.nctm.org/research/EdTech/
21 https://sails.deusto.es/

CONCLUSIONE

Le alleanze possono rafforzare le scuole, ma possono anche comprometterle. I dirigenti devono agire come guardiani vigili della sicurezza degli studenti e dell'integrità istituzionale.

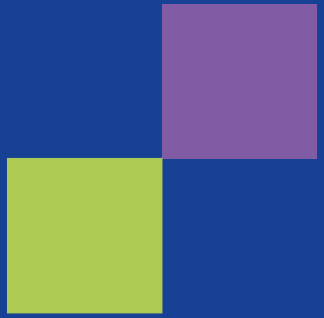
Attraverso:

- la valutazione delle partnership con occhio critico.
- la promozione delle relazioni digitali etiche.
- risposte trasparenti quando sorgono problemi.
- la costruzione di alleanze solide con insegnanti, studenti, genitori e comunità

I dirigenti possono garantire che ogni alleanza rafforzi, anziché indebolire, la missione dell'istruzione.

Partnership etiche, trasparenti ed eque non solo sviluppano l'alfabetizzazione digitale, ma anche la fiducia e la resilienza dell'intera comunità scolastica.

MODELLI DI LINEE GUIDA PER DIRIGENTI SCOLASTICI



1. MODELLO DI LINEE GUIDA CONTRO IL CYBERBULLISMO

Scopo

La presente politica definisce l'impegno della scuola nella prevenzione, nell'individuazione e nella gestione dei casi di bullismo e cyberbullismo, al fine di garantire un ambiente sicuro e rispettoso per tutti gli studenti e il personale.

Ambito

Il presente protocollo si applica a:

- Studenti, personale e genitori coinvolti in interazioni digitali relative alla scuola.
- Piattaforme online utilizzate per l'insegnamento, i compiti a casa, le attività extrascolastiche e le comunicazioni informali che riguardano la comunità scolastica.

Definizioni

- Bullismo: comportamento aggressivo ripetuto con l'intento di danneggiare o intimidire.
- Cyberbullismo: bullismo condotto attraverso mezzi digitali quali social media, app di messaggistica o giochi online.

Responsabilità

- Dirigenti: stabilire protocolli e procedure, fornire risorse e supervisionarne l'attuazione.
- Insegnanti: monitorare le interazioni tra gli studenti, dare l'esempio con un comportamento rispettoso, intervenire quando necessario.
- Studenti: segnalare gli incidenti e rispettare le linee guida sulla condotta digitale.
- Genitori: sostenere gli sforzi della scuola e rafforzare i comportamenti rispettosi a casa.

Procedura

1. Prevenzione:

- Educazione alla cittadinanza digitale inclusa nel programma scolastico.
- Campagne di sensibilizzazione organizzate ogni anno per studenti e genitori.

2. Segnalazione:

- Sono disponibili diversi canali: moduli anonimi, personale di fiducia, strumenti di segnalazione digitale.

3. Risposta:

- Incidenti documentati e indagati tempestivamente.
- Si dà priorità alle pratiche riparative, ma se necessario vengono intraprese azioni disciplinari.

4. Supporto:

- Le vittime ricevono consulenza e sostegno da parte del personale.
- Ai responsabili viene offerta una guida per modificare il loro comportamento.

Revisione

Questo protocollo sarà rivisto ogni due anni, con il contributo del personale, dei genitori e del corpo studentesco. HEADstart #25 sottolinea l'importanza di una politica organizzativa coerente, che si applica anche ai documenti relativi al digitale. Una revisione congiunta di tutte le politiche digitali, di salvaguardia e di partnership, insieme al responsabile della protezione dei dati e ai rappresentanti del personale, contribuisce a garantire che la terminologia, i principi etici e i riferimenti giuridici siano coerenti in tutta la scuola.

2. SCHEMA DEL QUADRO DI RIFERIMENTO PER L'ALFABETIZZAZIONE DIGITALE

Scopo

Garantire che tutti gli studenti e il personale sviluppino solide competenze di alfabetizzazione digitale, consentendo loro di valutare criticamente, utilizzare e creare contenuti digitali in modo responsabile.

Competenze fondamentali

1. Alfabetizzazione informatica: capacità di trovare, valutare e utilizzare fonti affidabili.
2. Pensiero critico: mettere in discussione i contenuti digitali e riconoscere i pregiudizi.
3. Resilienza digitale: affrontare sfide quali il cyberbullismo o l'esposizione a contenuti dannosi.
4. Consapevolezza della sicurezza informatica: proteggere i dati personali e scolastici.
5. Uso etico: rispetto della proprietà intellettuale, della privacy e dei diritti digitali.

Attuazione

- Integrazione nel programma scolastico: alfabetizzazione digitale inclusa in tutte le materie.
- Sviluppo professionale: formazione continua per gli insegnanti.
- Cultura scolastica complessiva: poster, assemblee e pratiche condivise che promuovono l'impegno critico.

Valutazione

- Portfolio degli studenti che documentano i progetti digitali.
- Riflessioni degli insegnanti e revisioni tra pari.
- Revisione annuale dei risultati di alfabetizzazione digitale da parte della dirigenza scolastica.

3. LINEE GUIDA SCOLASTICHE IN MERITO ALLA CYBERSECURITY

Scopo

Proteggere l'infrastruttura digitale della scuola e salvaguardare i dati sensibili appartenenti a studenti, personale e genitori.

Pratiche chiave

- Password: sono richieste password complesse e uniche, aggiornate annualmente.
- Autenticazione: autenticazione a due fattori per gli account del personale.
- Aggiornamenti software: aggiornamenti regolari e patch di tutti i sistemi scolastici.
- Backup: backup sicuri e regolari dei dati essenziali.
- Gestione dei dispositivi: regole chiare per i dispositivi di proprietà della scuola e quelli personali.

Ruoli e responsabilità

- Dirigenza scolastica: garantire un budget adeguato e una formazione adeguata in materia di sicurezza informatica.
- Personale IT: mantenere sistemi sicuri, condurre audit regolari e rispondere agli incidenti.
- Insegnanti e personale: seguire i protocolli di sicurezza, segnalare attività sospette.
- Studenti: utilizzare i dispositivi in modo responsabile e seguire le linee guida di sicurezza.

Risposta agli incidenti

1. Rilevare e segnalare: qualsiasi sospetta violazione deve essere segnalata immediatamente.
2. Contenere: isolare i sistemi interessati.
3. Indagare: il personale IT valuta l'entità e l'origine della violazione.
4. Comunicare: informare tempestivamente i genitori e il personale con aggiornamenti trasparenti.
5. Recupero: ripristino dei sistemi e dei dati da backup sicuri.
6. Riesaminare: identificare le lezioni apprese e aggiornare il protocollo.

4. LINEE GUIDA DI RISPOSTA ALLA DISINFORMAZIONE

Scopo

Stabilire una procedura chiara per affrontare i casi di disinformazione o informazioni errate che interessano la comunità scolastica.

Fattori scatenanti

- Informazioni false che circolano sul personale, sugli studenti o sulle azioni amministrative scolastiche. Dicerie sui social media che incidono sulla fiducia o sulla sicurezza.

Passi

1. Monitoraggio: designare il personale incaricato di seguire le questioni emergenti.
2. Verificare: confermare rapidamente i fatti con fonti affidabili.
3. Comunicare: condividere aggiornamenti tempestivi e accurati con il personale, i genitori e gli studenti tramite i canali ufficiali.
4. Educare: utilizzare l'incidente come opportunità didattica per rafforzare l'alfabetizzazione mediatica.
5. Portare al livello successivo: coinvolgere le autorità locali o i media se la disinformazione causa danni significativi.

5. LINEE GUIDA PER ALLEANZE E PARTNERSHIP

Scopo

Garantire che le partnership scolastiche con fornitori di tecnologia, piattaforme e aziende esterne tutelino il benessere degli studenti e siano in linea con gli standard etici.

Principi

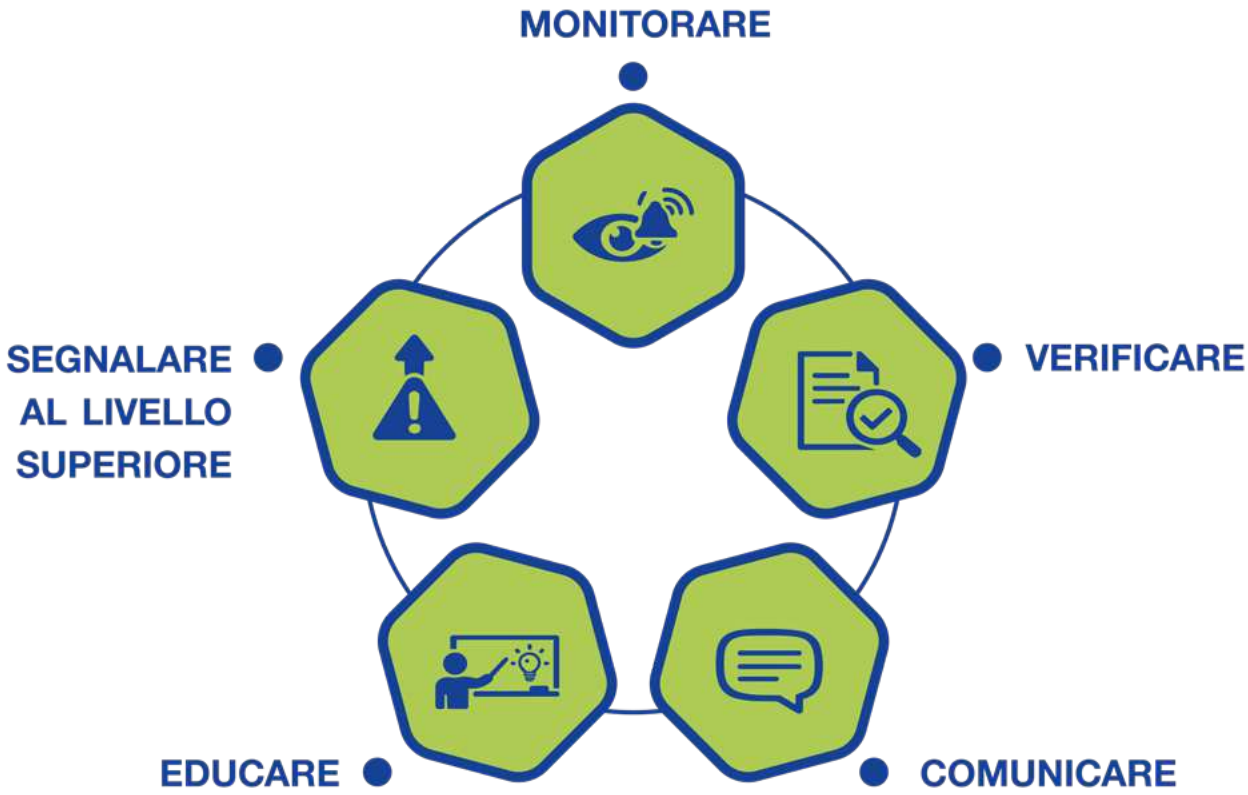
- Trasparenza: contratti e partnership spiegati chiaramente ai genitori e al personale.
- Privacy: nessuna raccolta o utilizzo non necessario dei dati degli studenti.
- Responsabilità: i partner devono rispettare gli standard nazionali e internazionali in materia di protezione dei minori.

Procedura

- Rivedere tutti i contratti con consulenti legali/informatici.
- Coinvolgere i genitori e il personale nelle discussioni sulle nuove piattaforme.
- Verificare annualmente la conformità delle partnership agli standard di privacy ed etica.

Esempio: una scuola valuta una nuova piattaforma di e-learning. Prima dell'adozione, il team dirigenziale verifica le pratiche di raccolta dei dati, informa i genitori e garantisce la conformità al GDPR.

PROTOCOLLO DI RISPOSTA ALLA DISINFORMAZIONE



STRUMENTI

FORMAZIONE DELLE COMPETENZE PROFESSIONALI

Iniziate da voi stessi

L'alfabetizzazione digitale e la resilienza non sono solo materie da insegnare, ma competenze professionali. La ricerca condotta da DRONE e da progetti correlati dimostra che i professionisti che non hanno sviluppato le proprie competenze spesso:

- hanno difficoltà nel definire modelli di buone pratiche per gli studenti.
- si sentono sopraffatti dalle nuove sfide (ad esempio, tendenze alla disinformazione, rischi per la sicurezza informatica).
- mancano di fiducia nelle proprie capacità di guidare un cambiamento significativo a livello scolastico.

Principio chiave: non è possibile insegnare efficacemente ciò che non si è ancora padroneggiato personalmente.

Fase 1: Valutate la vostra alfabetizzazione digitale

Prima di implementare programmi per gli studenti, i professionisti dovrebbero valutare il proprio punto di partenza. Questo aiuta a identificare i punti di forza e le aree di crescita.

Esempio di test di autovalutazione (insegnanti/dirigenti)

Valutatevi da 1 (non sicuro) a 5 (molto sicuro).

1. Sono in grado di riconoscere quando le informazioni online sono parziali o incomplete.
2. Sono in grado di utilizzare almeno due diversi metodi di verifica dei fatti (ad esempio, ricerca inversa delle immagini, siti di verifica dei fatti).
3. Conosco la differenza tra disinformazione, informazioni errate e satira.
4. Sono in grado di spiegare le impostazioni sulla privacy e le nozioni di base sulla sicurezza informatica a colleghi e studenti.
5. Mi sento sicuro nel rispondere a un genitore o a uno studente che condivide informazioni false o fuorvianti.
6. Sono in grado di gestire il mio benessere digitale (ad esempio, equilibrio, gestione della negatività online).
7. Comprendo come i contratti con le piattaforme digitali possano influire sui dati degli studenti.

Punteggio:

- 30-35 = Competenza elevata. Pronto a dare l'esempio e a guidare gli altri.
- 20–29 = Competenza moderata. Identificare le aree per una formazione mirata.
- Meno di 20 = Necessità di un supporto significativo prima di insegnare agli altri.

Fase 2: Percorsi di sviluppo professionale

- Corsi brevi: partecipare a moduli asincroni (ad esempio, corso online DRONE, programma di alfabetizzazione mediatica dell'UNESCO).
- Apprendimento tra pari: creare comunità di apprendimento professionale in cui gli insegnanti si esercitano nella verifica dei fatti o condividono strategie di resilienza.
- Formazione esterna: partecipare a workshop organizzati da organizzazioni affidabili (OCSE, European Schoolnet, Common Sense Education).
- Diari di riflessione: tenere un diario digitale delle sfide affrontate e delle strategie apprese.

Fase 3: Riflessione continua e modellizzazione

- Siate trasparenti con gli studenti riguardo al vostro processo di apprendimento.
- Condividete online le vostre esperienze personali relative agli errori commessi: questo promuove la riflessione critica.
- Aggiornate regolarmente le vostre competenze man mano che le piattaforme, gli strumenti e i rischi evolvono.



CASO DI STUDIO: "GESTIRE IMPARANDO PRIMA"

Il dirigente di una scuola si è reso conto che il personale non era sicuro di sé nell'insegnamento delle fake news. Prima di lanciare un programma per gli studenti, ha organizzato una formazione di due giorni per il personale, durante la quale gli insegnanti si sono esercitati a identificare la disinformazione, hanno sostenuto dei test di autovalutazione e hanno riflettuto sulle proprie abitudini online. Solo dopo questo la scuola ha introdotto un'iniziativa rivolta agli studenti. Il personale ha riferito di sentirsi più responsabilizzato e autentico come modello di riferimento.

Passaggio 4: mappate il flusso delle vostre informazioni

Disegnate una linea temporale giornaliera e includete tutte le fonti di informazioni digitali con cui avete interagito (ad esempio WhatsApp, siti di notizie, e-mail scolastiche, Instagram, ecc.)

Domande di riflessione:

- Quali modelli notate?
- Quali fonti ritenete più affidabili?
- Quali fonti ritenete meno affidabili?

AFFRONTARE IL BULLISMO COMMESSO DAGLI INSEGNANTI

Perché è importante

Sebbene molta attenzione sia giustamente rivolta al bullismo tra pari, la ricerca DRONE e studi internazionali rivelano una lacuna critica: gli studenti possono subire bullismo anche da parte degli insegnanti o di altro personale scolastico. Ciò può comportare:

- Umiliazioni davanti ai compagni.
- Vessazioni ingiuste o ripetute.
- Abuso di potere nella valutazione, nella disciplina o nelle dinamiche di classe.
- Molestie online o comunicazioni digitali inappropriate.

Tali esperienze sono profondamente dannose. Minano la fiducia nell'istruzione, danneggiano il benessere e costituiscono un cattivo esempio per gli studenti.

Misure preventive per i dirigenti

- Politica di tolleranza zero: chiarire che il bullismo da parte del personale è inaccettabile e comporta conseguenze.
- Codice di condotta: includere un comportamento rispettoso sia online che di persona nelle politiche del personale.
- Sistemi di segnalazione riservati: garantire che gli studenti (e i genitori) possano segnalare in modo sicuro il bullismo da parte degli insegnanti.
- Formazione regolare: includere moduli sulle dinamiche di potere, l'empatia e la comunicazione digitale appropriata.
- Osservazione e responsabilità: utilizzare osservazioni tra pari, sondaggi tra gli studenti, visite di controllo da parte della dirigenza per individuare i primi segnali di allarme.

Misure preventive per gli insegnanti

- Pratica riflessiva: chieditevi regolarmente: "Le mie parole o azioni potrebbero essere percepite come umilianti o rivolte contro uno studente?"
- Consapevolezza linguistica: evitate il sarcasmo, l'umiliazione pubblica o i confronti che mettono in risalto negativamente alcuni studenti.
- Disciplina con dignità: applicate le regole in modo coerente, spiegate il vostro ragionamento ed evitate attacchi personali.

- Confini digitali: mantenete tutte le vostre comunicazioni online con gli studenti professionali, trasparenti e approvate dalla scuola.

QUANDO LE COSE VANNO MALE

Se un insegnante viene accusato di bullismo nei confronti di uno studente:

- Risposta immediata: prendere sul serio l'accusa; assicurarsi che lo studente si senta al sicuro.
- Indagine: la direzione scolastica deve condurre un'indagine tempestiva, equa e riservata.
- Sostegno: fornire sostegno emotivo allo studente. Offrire misure di formazione professionale all'insegnante, a seconda della gravità.
- Pratiche riparative: ove possibile, ricorrere al dialogo riparativo per ricostruire la fiducia.



CASO DI STUDIO 1: "L'INSEGNANTE SARCASTICO"

Un insegnante di scuola secondaria prendeva spesso in giro gli studenti per le risposte sbagliate. Uno studente ha iniziato a saltare le lezioni, dichiarandosi malato. I genitori hanno segnalato il problema. La dirigente ha condotto colloqui riservati, confermando il comportamento. All'insegnante è stato richiesto di frequentare un corso di formazione sulla comunicazione in classe ed è stato affiancato da un collega più esperto.
È stato organizzato un incontro di mediazione con lo studente coinvolto. Lo studente è tornato in classe e l'insegnante ha segnalato una maggiore consapevolezza dell'uso del linguaggio.

CASO DI STUDIO 2: "SUPERARE I LIMITI DIGITALI"

Un insegnante ha utilizzato un'app di messaggistica privata per contattare studenti in merito ai compiti, inviando talvolta messaggi critici a tarda notte. Gli studenti si sono sentiti sotto pressione e umiliati. La scuola ha indagato e stabilito una nuova politica: tutte le comunicazioni digitali devono passare attraverso la piattaforma ufficiale della scuola. È stata fornita una formazione sui confini digitali.

Punti Chiave per Insegnanti e Dirigenti

1. Sviluppate prima voi stessi: l'alfabetizzazione digitale inizia con l'auto-riflessione e lo sviluppo delle competenze.

2. Misurate e migliorate – Utilizzate autovalutazioni per identificare le vostre aree di crescita.

3. Date l'esempio – gli studenti e il personale imparano soprattutto da ciò che fate, non solo da ciò che dite.

4. Affrontate tutte le forme di bullismo – Compreso il problema spesso nascosto del bullismo da parte degli insegnanti nei confronti degli studenti.

5. Create sistemi sicuri: segnalazioni, indagini e supporto devono essere trasparenti e affidabili.

CHECKLIST PER LA FORMAZIONE PERSONALE

Parte 1: Autovalutazione delle competenze digitali per professionisti

Istruzioni

Questo autotest vi aiuta a identificare i vostri punti di forza e le aree di crescita in materia di alfabetizzazione digitale prima di insegnare o implementare programmi educativi.

- Valutatevi da 1 (per niente sicuro) a 5 (molto sicuro).
- Siate sinceri: questo è per riflettere su voi stessi, non per essere valutati da altre persone.

Sezione A: Alfabetizzazione informatica

1. Sono in grado di valutare la credibilità di un articolo o di un video online. ☐
2. Sono in grado di identificare lo scopo e il bias dietro una fonte. ☐
3. Utilizzo strumenti di verifica dei fatti (ad esempio, ricerca per immagini, Snopes, Full Fact). ☐
4. Sono in grado di insegnare ad altre persone a confrontare efficacemente più fonti. ☐

Punteggio A: ___ / 20

Sezione B: Consapevolezza della disinformazione

5. Sono in grado di spiegare la differenza tra disinformazione, misinformazione e satira. ☐
6. Riconosco i segnali di allarme comuni delle fake news. ☐
7. Sono in grado di rispondere in modo costruttivo quando qualcuno condivide informazioni errate. ☐
8. Mi tengo informato sulle attuali tendenze in materia di disinformazione ☐

Punteggio B: ___ / 20 ☐

Sezione C: Resilienza e risoluzione dei problemi

9. Conosco strategie per affrontare la negatività o le molestie online. ☐
10. Mi sento sicuro nel trasmettere resilienza a colleghi e studenti. ☐
11. Sono in grado di guidare studenti attraverso i dilemmi digitali utilizzando un approccio strutturato alla risoluzione dei problemi. ☐
12. Mantengo un sano equilibrio tra la mia vita online e quella offline. ☐

Punteggio C: ___ / 20

Sezione D: Pensiero critico

13. Analizzo regolarmente le prove e identifico i pregiudizi nei contenuti digitali. ☐
14. Integro pratiche di pensiero critico nella mia attività di insegnamento. ☐
15. Sono in grado di aiutare gli studenti a valutare informazioni contrastanti. ☐
16. Sono in grado di individuare quando contenuti complottisti o estremisti influenzano le discussioni in classe ☐

Punteggio D: ___ / 20

Sezione E: Cybersecurity

17. Utilizzo password complesse e uniche e l'autenticazione a due fattori. ☐
18. Mantengo aggiornati i dispositivi e i software. ☐
19. Riconosco i segnali di tentativi di phishing o truffe. ☐
20. So come proteggere i dati degli studenti in classe. ☐

Punteggio E: ___ / 20

Guida alla valutazione

80–100: Competenza elevata. Pronto per essere un esempio e una guida.

60–79: Competenza moderata. Identificare le possibili aree di miglioramento.

40–59: Competenze di base. Si raccomanda un approfondimento professionale significativo.

Meno di 40: È assolutamente necessario seguire una formazione strutturata prima di insegnare queste competenze agli studenti.

Spunti di riflessione

- In quali aree ho ottenuto il punteggio più basso?
- Come potrei migliorare tali competenze nei prossimi 6 mesi?
- Quale formazione, supporto da parte dei colleghi o risorse mi sarebbero più utili?

Parte 2: Checklist per la prevenzione del bullismo per il personale

Scopo

Prevenire ogni forma di bullismo, compreso quello spesso trascurato tra insegnanti e studenti.

Per gli insegnanti (autovalutazione)

- Uso un linguaggio rispettoso anche quando correggo gli errori. ☐
- Evito il sarcasmo, la derisione o l'umiliazione pubblica. ☐
- Applico la disciplina in modo coerente ed equo. ☐
- Mi chiedo spesso: le mie azioni potrebbero essere interpretate come rivolte contro uno studente? ☐
- Mantengo professionali e trasparenti tutte le comunicazioni digitali con gli studenti. ☐
- Chiedo ai colleghi o ai mentori un parere sul mio modo di gestire la classe. ☐
- So come comportarmi se assistessi a un episodio di bullismo da parte di un collega nei confronti di uno studente. ☐

Per i dirigenti (monitoraggio e supporto)

- Esiste un codice di condotta chiaro che include le interazioni tra insegnanti e studenti. ☐
- Sono stati istituiti sistemi di segnalazione riservati a disposizione di studenti e genitori. ☐
- Il personale riceve una formazione periodica in materia di empatia, comunicazione e dinamiche di potere. ☐
- Le osservazioni in classe o i sondaggi tra gli studenti consentono di monitorare i rapporti tra il personale e gli studenti. ☐
- Le segnalazioni di episodi di bullismo da parte degli insegnanti vengono esaminate tempestivamente e in modo imparziale. ☐
- Viene fornito sostegno (consulenza, tutoraggio o formazione) sia alle vittime che al personale coinvolto. ☐
- Le procedure disciplinari sono chiare e vengono applicate quando necessario. ☐

Strumento di riflessione sui casi (per le riunioni del personale)

- Descrivi una situazione in cui uno studente si è sentito preso di mira da un insegnante.
- Come si sarebbe potuta gestire la situazione in modo diverso?
- Quali misure di sicurezza potrebbero impedire che ciò si ripeta?

PIANO DI SVILUPPO PROFESSIONALE PER INSEGNANTI E DIRIGENTI SCOLASTICI

Fase 1: Base di riferimento e consapevolezza (mesi 1-2)

Obiettivi

- Stabilire una chiara comprensione degli attuali livelli di competenza.
- Sensibilizzare sui rischi legati all'alfabetizzazione digitale, alla disinformazione e al bullismo.

Azioni

- Somministrare il test di autovalutazione delle competenze digitali a tutto il personale.
- Raccogliere i risultati in forma anonima per identificare i punti di forza e le lacune dell'intera scuola.
- Organizzare un workshop introduttivo dal titolo: "Perché l'alfabetizzazione digitale e la resilienza sono importanti per le scuole".
- Condividere casi di studio tratti dai manuali DRONE per illustrare le sfide reali.

Risultati

- Rapporto di riferimento sulle competenze del personale.
- Sensibilizzazione del personale e della dirigenza.

Fase 2: Sviluppo delle competenze personali (mesi 3-5)

Obiettivi

- Rafforzare le competenze individuali prima di insegnare agli studenti.
- Incoraggiare la riflessione e la responsabilità personale.

Azioni

- Offrire brevi corsi online (ad esempio, moduli asincroni DRONE, corso MIL dell'UNESCO https://www.unesco.org/en/media-information-literacy/moocs).
- Organizzare gruppi di apprendimento tra pari: gli insegnanti si esercitano nella verifica dei fatti, identificano le fake news e riflettono sulla resilienza digitale.

- Fornire accesso a liste di letture consigliate e toolkit.
- Incoraggiare ogni insegnante a fissare un obiettivo personale in materia di competenze digitali (ad esempio, padroneggiare la ricerca per immagini, migliorare la sicurezza delle password).

Risultati

- Il personale aumenta la propria fiducia nelle competenze digitali.
- Creazione di reti di supporto tra pari.

Fase 3: Progetti pilota di integrazione in classe (mesi 6-8)

Obiettivi

- Iniziare a sperimentare l'integrazione dell'alfabetizzazione digitale nell'insegnamento.
- Concentrarsi sulle competenze di modellazione, non ancora sui programmi completi.

Azioni

- Gli insegnanti sperimentano 1-2 attività didattiche tratte dal Toolkit per la pianificazione delle lezioni (ad esempio, l'esercizio di individuazione delle fake news).
- I dirigenti organizzano sessioni di riflessione per condividere successi e sfide.
- Viene introdotta la checklist per la prevenzione del bullismo, ponendo l'accento sul comportamento degli insegnanti nei confronti degli studenti.
- Raccogliere i feedback degli studenti sulle lezioni pilota: cosa ha funzionato? Cosa li ha confusi?

Risultati

- Prime prove di come si presenta l'integrazione nella pratica.
- Consapevolezza del personale riguardo al linguaggio e al comportamento degli studenti.

Fase 4: Implementazione in tutte le attività scolastiche (mesi 9-10)

Obiettivi

- Integrare l'alfabetizzazione digitale nella cultura e nel programma scolastico.
- Stabilire politiche e sistemi a sostegno del lavoro a lungo termine.

Azioni

- Finalizzare e adottare un quadro di riferimento per l'alfabetizzazione digitale nella scuola
- Lanciare campagne di sensibilizzazione a livello scolastico (assemblee, poster, newsletter per i genitori).
- Attuare politiche anti-bullismo che includano esplicitamente le dinamiche tra il personale e gli studenti.
- Organizzare seminari sulla resilienza sia per il personale che per gli studenti.

Risultati

- Alfabetizzazione digitale integrata in diverse materie.
- Attuazione di una politica anti-bullismo a livello scolastico.
- Cultura condivisa di resilienza e impegno critico.

Fase 5: Revisione e consolidamento (mesi 11-12)

Obiettivi

- Misurare i progressi e perfezionare le pratiche.
- Garantire la sostenibilità dello sviluppo professionale.

Azioni

- Somministrare nuovamente il test di autovalutazione delle competenze digitali a tutto il personale.
- Confrontare i risultati con quelli di riferimento per monitorare la crescita.
- Raccogliere casi di studio di iniziative scolastiche e di classe che hanno funzionato.
- Aggiornare il piano di sviluppo professionale per l'anno successivo.

Risultati

- Rapporto di valutazione che mostra la crescita delle competenze.
- Piano d'azione perfezionato per il secondo anno (maggiore attenzione alla sicurezza informatica, alle alleanze con le aziende e alle partnership con i genitori).

Supporto continuo durante tutto l'anno

- Coaching tra pari: incontri mensili in piccoli gruppi in cui gli insegnanti si sostengono a vicenda.
- Controlli sulla leadership: sondaggi trimestrali tra il personale per monitorare la cultura digitale.
- Voce degli studenti: meccanismi di feedback che consentono agli studenti di riflettere sulle lezioni di alfabetizzazione digitale e sul comportamento degli insegnanti.
- Coinvolgimento dei genitori: workshop e newsletter per allineare gli approcci della scuola e della famiglia.

Caso di studio: una trasformazione in un anno

All'inizio dell'anno, una scuola secondaria ha scoperto che il 65% del personale aveva

ottenuto un punteggio inferiore a “competenza moderata” nel test di autovalutazione. Gli studenti hanno segnalato informazioni errate in classe e occasionali episodi di sarcasmo da parte di insegnanti che sono degenerati in denunce di bullismo.

Alla fine del percorso:

- I nuovi test del personale hanno mostrato un aumento medio del 25% della fiducia in tutti i settori.
- Un nuovo quadro di riferimento per l’alfabetizzazione digitale è stato integrato nei corsi di inglese, scienze e studi sociali.
- Il feedback degli studenti ha evidenziato che si sentivano più sicuri nel discutere in classe delle difficoltà incontrate online.
- È stato adottato un codice anti-bullismo chiaro sia per il personale che per gli studenti.

GUIDA DI RIFERIMENTO RAPIDO PER I DIRIGENTI

(Un complemento al Manuale per dirigenti scolastici DRONE)

1. Alfabetizzazione digitale e disinformazione: priorità della dirigenza

Il vostro ruolo di dirigente

- Create una cultura scolastica basata sul pensiero critico e sulla sicurezza.
- Date l'esempio di un comportamento digitale responsabile nelle vostre comunicazioni.
- Fornite strutture, politiche e formazione chiare al personale.
- Coinvolgete genitori e studenti in conversazioni aperte sulle difficoltà provenienti dal mondo digitale.

Segnali di allarme

- Il personale non sa come reagire alle fake news o alle notizie non verificate che circolano in rete.
- I genitori diffidano delle comunicazioni della scuola a causa della disinformazione.
- Gli studenti ripetono affermazioni non verificate o estreme senza metterle in discussione.

2. Alfabetizzazione informatica

Azioni della dirigenza

- Integrare le competenze di verifica delle fonti e di valutazione in tutto il programma di studi.
- Supportare gli insegnanti con strategie di verifica dei fatti pronte per l'uso in classe.
- Fornire formazione al personale sulla gestione della misinformazione

Segnali di allarme

- Insegnanti che si affidano a un'unica fonte online per il materiale didattico.
- Studenti che faticano a distinguere i fatti dalle opinioni.
- Controversie a scuola scatenate da dicerie o affermazioni non verificate.

3. Sviluppo della resilienza

Azioni della dirigenza

- Formare il personale a individuare i primi segni di disagio digitale.
- Fornire consulenza e sistemi di supporto tra pari per studenti.
- Promuovere il benessere digitale (pause dallo schermo, confini salutari).

Segnali di allarme

- Personale che mostra segni di esaurimento dovuto al sovraccarico digitale.
- Studenti che evitano i dispositivi a causa dell'ansia.
- Conflitti online sempre più accesi che si riversano nella vita scolastica.

4. Risoluzione dei problemi in un mondo digitale

Azioni della dirigenza

- Incoraggiare soluzioni creative ai dilemmi digitali.
- Fornire formazione professionale al personale nella risoluzione dei conflitti online.
- Coinvolgere gli studenti nella definizione delle politiche digitali della scuola.

Segnali di allarme

- Gli insegnanti che aggravano i conflitti digitali invece di attenuarli.
- Gli studenti si disimpegnano quando sorgono problemi digitali.
- Mancanza di chiarezza su "cosa fare" in caso di problemi online.

5. Pensiero critico

Azioni della dirigenza

- Promuovere una cultura del dubbio: "Chi ha scritto questo? Perché? Cosa manca?"
- Integrare il pensiero critico in tutte le materie, non solo in quelle relative all'ICT.
- Supportare gli insegnanti con strumenti e risorse da utilizzare in classe.

Segnali di allarme

- Studenti (o personale) che credono e diffondono teorie complottiste.

- Discussioni in classe interrotte invece che approfondite in modo critico.
- Il personale non si sente a proprio agio nel porre domande critiche.

6. Bullismo e cyberbullismo

Azioni della dirigenza

- Stabilire politiche di tolleranza zero per tutti i tipi di bullismo, da parte di insegnanti, familiari o coetanei.
- Creare canali di segnalazione riservati per studenti e genitori.
- Formare il personale alla gestione delle prove digitali (screenshot, messaggi).
- Adottare approcci riparativi quando è sicuro farlo, ma agire con fermezza quando il danno è grave.

Segnali di allarme

- Segnalazioni di umiliazioni tra insegnanti e studenti liquidate come “disciplina”.
- Bullismo familiare ignorato perché avviene “a casa”.
- Video virali o molestie online che causano danni alla reputazione.

7. Cybersecurity

Azioni della dirigenza

- Richiedere una formazione annuale del personale (sensibilizzazione al phishing, igiene delle password).
- Garantire backup offline dei sistemi critici.
- Disporre di un piano di risposta agli incidenti collaudato in caso di violazioni.
- Insegnare agli studenti pratiche di sicurezza informatica adeguate alla loro età.
- Coinvolgere i genitori nella sensibilizzazione alla sicurezza informatica domestica.

Segnali di allarme

- Il personale utilizza la stessa password per più sistemi.
- Dispositivi personali non protetti collegati alle reti scolastiche.
- Mancanza di una procedura chiara per segnalare e-mail sospette.

8. Creare alleanze

Azioni della leadership

- Esaminare attentamente ogni contratto: proprietà dei dati, trasparenza, strategia di uscita
- Dare priorità a partnership etiche che tutelino gli studenti.
- Coinvolgere insegnanti, genitori e studenti nella valutazione degli strumenti digitali.
- Costruire alleanze con organizzazioni comunitarie, università e ONG.

Segnali di allarme

- App “gratuite” che monetizzano i dati degli studenti
- Sponsor che esercitano pressioni sulla scuola per promuovere i propri prodotti.
- Genitori che scoprono una condivisione nascosta dei dati a loro insaputa.

Checklist di Risposta alle Crisi

Quando un incidente digitale si aggrava (dicerie, violazione dei dati, cyberbullismo):

1. Contenere: fermate il danno immediato. ☐
2. Verificare: raccogliete i fatti prima di parlare. ☐
3. Comunicare: informate con chiarezza il personale, i genitori, gli studenti. ☐
4. Sostenere: fornite consulenza o assistenza a chi è stato colpito. ☐
5. Rivedere: aggiornate le linee guida e la formazione per prevenire il ripetersi dell’evento. ☐

Le 10 abitudini di leadership più importanti per una scuola digitalmente sicura

1. Utilizzate password forti e uniche (o un gestore di password).
2. Mantenete i vostri dispositivi sicuri e aggiornati.
3. Definite chiaramente le aspettative sulla cybersecurity con il personale e gli studenti.
4. Rivedete tutti i contratti esterni con consulenti legali e di sicurezza.
5. Organizzate corsi di formazione annuali di alfabetizzazione digitale e cybersecurity per il personale.
6. Coinvolgete genitori e studenti nella definizione delle linee guida.
7. Promuovete canali di segnalazione aperti per casi di bullismo o problemi online.
8. Date l’esempio in materia di trasparenza e comunicazione responsabile.
9. Eseguite regolarmente il backup dei dati e testate i sistemi di ripristino.
10. Festeggiate i successi ottenuti in materia di resilienza digitale e pensiero critico.

ALLEGATI

ALLEGATO 1

5 Aree del Quadro delle competenze digitali per i cittadini (DigComp)

Il Quadro delle competenze digitali per i cittadini (DigComp) è uno strumento di riferimento a livello europeo progettato per fornire una visione comune delle aree chiave delle competenze digitali. Supporta i responsabili politici nella progettazione di iniziative e aiuta a pianificare programmi di istruzione e formazione volti a migliorare le competenze digitali di gruppi specifici e a migliorare le competenze digitali complessive dei cittadini. L'ultima edizione, DigComp 3.0, aggiorna il quadro per riflettere i recenti sviluppi nell'ambito dell'intelligenza artificiale, della sicurezza informatica, dei diritti digitali e del benessere, e introduce nuovi risultati di apprendimento per una descrizione più dettagliata delle competenze. Definisce la competenza digitale come «l'uso sicuro, critico e responsabile delle tecnologie digitali per l'apprendimento, il lavoro e la partecipazione alla società» (Cosgrove & Cachia, 2025) e la organizza in cinque aree di competenza: ricerca, valutazione e gestione delle informazioni; comunicazione e collaborazione; creazione di contenuti; sicurezza, benessere e uso responsabile (compreso l'impatto ambientale); identificazione e risoluzione dei problemi.

Definizione di competenza digitale

In DigComp 3.0, la competenza digitale implica "l'uso sicuro, critico e responsabile delle tecnologie digitali e il loro impiego nell'apprendimento, nel lavoro e nella partecipazione alla società. È definita come una combinazione di conoscenze, abilità e attitudini" (Raccomandazione del Consiglio sulle competenze chiave per l'apprendimento permanente, 2018).

Aree di competenza



DigComp 3.0 identifica le componenti chiave della competenza digitale in 5 aree di competenza:

1. Ricerca, valutazione e gestione delle informazioni

definire le esigenze informative e utilizzare strumenti digitali per cercare, individuare e recuperare informazioni e contenuti. Ciò include valutare la pertinenza e la credibilità (anche quando sono coinvolti sistemi di intelligenza artificiale) e organizzare, archiviare e gestire dati e informazioni digitali in modo strutturato.

2. Comunicazione e collaborazione

Interagire, condividere, comunicare e collaborare utilizzando le tecnologie digitali, con consapevolezza della diversità. Ciò comprende la partecipazione a servizi digitali pubblici e privati, l'esercizio della cittadinanza e dei diritti digitali e la gestione responsabile della propria presenza, identità e reputazione digitali.

3. Creazione di contenuti

Creare e modificare contenuti digitali in diversi formati e integrare o rielaborare le informazioni esistenti in una base di conoscenze più ampia. Ciò include la comprensione e l'applicazione del diritto d'autore e delle licenze, l'agire in modo etico durante la creazione o l'utilizzo di contenuti (anche tramite strumenti di AI) e l'applicazione di concetti di base di pensiero computazionale e programmazione.

4. Sicurezza, benessere e uso responsabile

Proteggere dispositivi, contenuti digitali, dati personali e privacy negli ambienti online, riconoscere e rispondere a rischi quali truffe, cyberbullismo o contenuti dannosi. Quest'area comprende anche il sostegno al benessere fisico, mentale e sociale negli ambienti digitali, la promozione dell'inclusione e la comprensione dell'impatto ambientale delle tecnologie digitali per incoraggiarne un uso più sostenibile.

5. Identificazione e risoluzione dei problemi

Identificare e valutare le esigenze e i problemi negli ambienti digitali e utilizzare strumenti digitali per rispondere in modo efficace. Ciò include la risoluzione di problemi tecnici e concettuali, l'adattamento degli ambienti digitali a esigenze specifiche, l'uso creativo delle tecnologie per migliorare i processi o sviluppare nuove soluzioni e il mantenimento di un aggiornamento costante sugli sviluppi digitali in corso e sulle loro implicazioni.

Il modello concettuale di riferimento DigComp

In DigComp 3.0, la competenza digitale è organizzata in cinque aree di competenza e 21 competenze. Insieme, queste aree di competenza e competenze formano il modello di riferimento concettuale del quadro. Inoltre, DigComp 3.0 descrive quattro livelli di competenza (base, intermedio, avanzato e altamente avanzato) e fornisce descrizioni delle competenze e risultati di apprendimento dettagliati per ciascuna competenza e livello.



ALLEGATO 2

Elenco di letture consigliate

1. Saggistica: Alfabetizzazione digitale, media e genitorialità

- "Digital Literacy Unpacked" di Katherine Schulten & Renee Hobbs

Strategie pratiche per insegnare e modellare l'alfabetizzazione mediatica critica.

- "Ten Arguments for Deleting Your Social Media Accounts Right Now" di Jaron Lanier

Uno sguardo lucido su come le piattaforme digitali manipolano il comportamento.

- "The Shallows: What the Internet Is Doing to Our Brains" di Nicholas Carr

Esplora come la connettività costante cambi l'attenzione e l'apprendimento.

- "Raising Humans in a Digital World" di Diana Graber

Una guida incentrata sui genitori dedicata alla cittadinanza digitale e alla resilienza.

- "Mediated: How the Media Shapes Your World and the Way You Live in It" di Thomas de Zengotita

Come i media alterano la nostra comprensione della realtà.

- "Digital Minimalism" di Cal Newport

Strategie per ritrovare la concentrazione e un uso consapevole della tecnologia.

- "So You've Been Publicly Shamed" di Jon Ronson

Uno sguardo affascinante sulla reputazione digitale, la vergogna e la resilienza.

2. Saggistica: Disinformazione, propaganda e democrazia

- "Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics" di Yochai Benkler, Robert Faris, and Hal Roberts

Analisi approfondita di come la disinformazione si diffonde attraverso le piattaforme.

- "How Fascism Works: The Politics of Us and Them" di Jason Stanley

Mostra come le narrazioni manipolative guadagnino terreno nelle società.

- "Manufacturing Consent" di Edward S. Herman and Noam Chomsky

Opera classica sulla manipolazione dei media e il potere.

- "Blur: How to Know What's True in the Age of Information Overload" di Bill Kovach and Tom Rosenstiel

Strumenti per giornalisti e cittadini per valutare la credibilità delle informazioni.

3. Saggistica: sviluppo infantile, bullismo e benessere

- "Odd Girl Out: The Hidden Culture of Aggression in Girls" di Rachel Simmons

Importanti approfondimenti sul bullismo relazionale, sia offline che online.

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

Misure pratiche contro il bullismo e il cyberbullismo.

- “It’s Complicated: The Social Lives of Networked Teens” di Danah Boyd

Esplorazione basata sulla ricerca di come gli adolescenti navigano negli spazi digitali.

- “Stolen Focus” di Johann Hari

Esplora come l’attenzione sia frammentata nell’era digitale.

4. Narrativa: verità, identità e manipolazione

- “1984” di George Orwell

Un’analisi senza tempo della disinformazione, della propaganda e della sorveglianza.

- “Fahrenheit 451” di Ray Bradbury

Romanzo classico sulla censura, il pensiero critico e i mass media.

- “Brave New World” di Aldous Huxley

Come il piacere, la distrazione e la manipolazione plasmano la società.

- “The Circle” di Dave Eggers

Una satira agghiacciante su un mondo iperconnesso e basato sui dati.

- “Little Brother” di Cory Doctorow

Romanzo young adult sulla sorveglianza, la resistenza e l’attivismo digitale.

- “Feed” di M.T. Anderson

Esplorazione fantascientifica del controllo delle multinazionali e della dipendenza digitale.

- “Snow Crash” di Neal Stephenson

Romanzo cyberpunk dal ritmo serrato che tratta di informazioni, memi e realtà virtuale.

- “Neuromancer” di William Gibson

Il classico cyberpunk originale: identità, intelligenza artificiale e futuro digitale.

- “The Three-Body Problem” di Liu Cixin

Esplora la scienza, la tecnologia e la manipolazione della verità su scala globale.

- “Ready Player One” di Ernest Cline

Cultura pop e evasione digitale in un mondo virtuale: divertente ma con un monito.

5. Per i lettori più giovani (da condividere con bambini e adolescenti)

- “Click’d” di Tamara Ireland Stone

Un romanzo per ragazzi che parla di programmazione, app e conseguenze indesiderate.

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

Un fantasy che esplora la narrazione, i miti e la resilienza culturale.

- “Restart” di Gordon Korman

Sull’identità, le seconde possibilità e il modo in cui gli altri influenzano la nostra reputazione.

- “Holes” di Louis Sachar

Classico romanzo per ragazzi con insegnamenti sulla giustizia, la resilienza e la comunità.

- “The Wild Robot” di Peter Brown

Esplora la tecnologia, l’adattamento e l’empatia in un modo che i bambini adorano.

6. Guide pratiche e kit di strumenti

- Common Sense Media Parent Guides (online, gratuito)

Recensioni affidabili di app, film e strumenti digitali.

- EU Kids Online Reports

Ricerca sulle abitudini digitali dei bambini in Europa.

- UNICEF Child Online Protection Guidelines

Standard globali per la tutela dei bambini negli spazi digitali.

Questo elenco è stato concepito in modo tale che:

- I genitori possano approfondire la loro comprensione e condividere con bambini e ragazzi opere di narrativa adeguate alla loro età.
- Gli insegnanti possano utilizzare sia opere di finzione che saggistica nella pianificazione delle lezioni.
- I dirigenti scolastici possano collegare le decisioni politiche a ricerche più ampie.

ALLEGATO 3

Introduzione all'intelligenza artificiale e all'istruzione

Ogni giorno interagiamo con l'AI in modi che passano inosservati, sottolineando la sua presenza universale nella nostra vita digitale. Il testo predittivo sui nostri smartphone, che rende più veloce che mai scrivere "Sto arrivando!", i contenuti che le nostre piattaforme di streaming e social media preferite ci suggeriscono e i consigli sui prodotti a volte spaventosamente accurati dei siti di shopping online sono tutti esempi di AI che lavora dietro le quinte. Questi casi sono ottimi esempi delle più ampie applicazioni dell'AI: sta già semplificando e ottimizzando tutte le nostre vite, quindi perché non introdurla nelle aule scolastiche per continuare questa tendenza? Dopo tutto, è l'uso finale, ovvero il modo in cui applichiamo questa tecnologia, che ne determina realmente l'impatto sulla società.

Benvenuti nell'entusiasmante nuovo mondo dell'istruzione, dove l'intelligenza artificiale non è il cattivo di un romanzo di fantascienza, ma un utile alleato nel mondo di oggi!

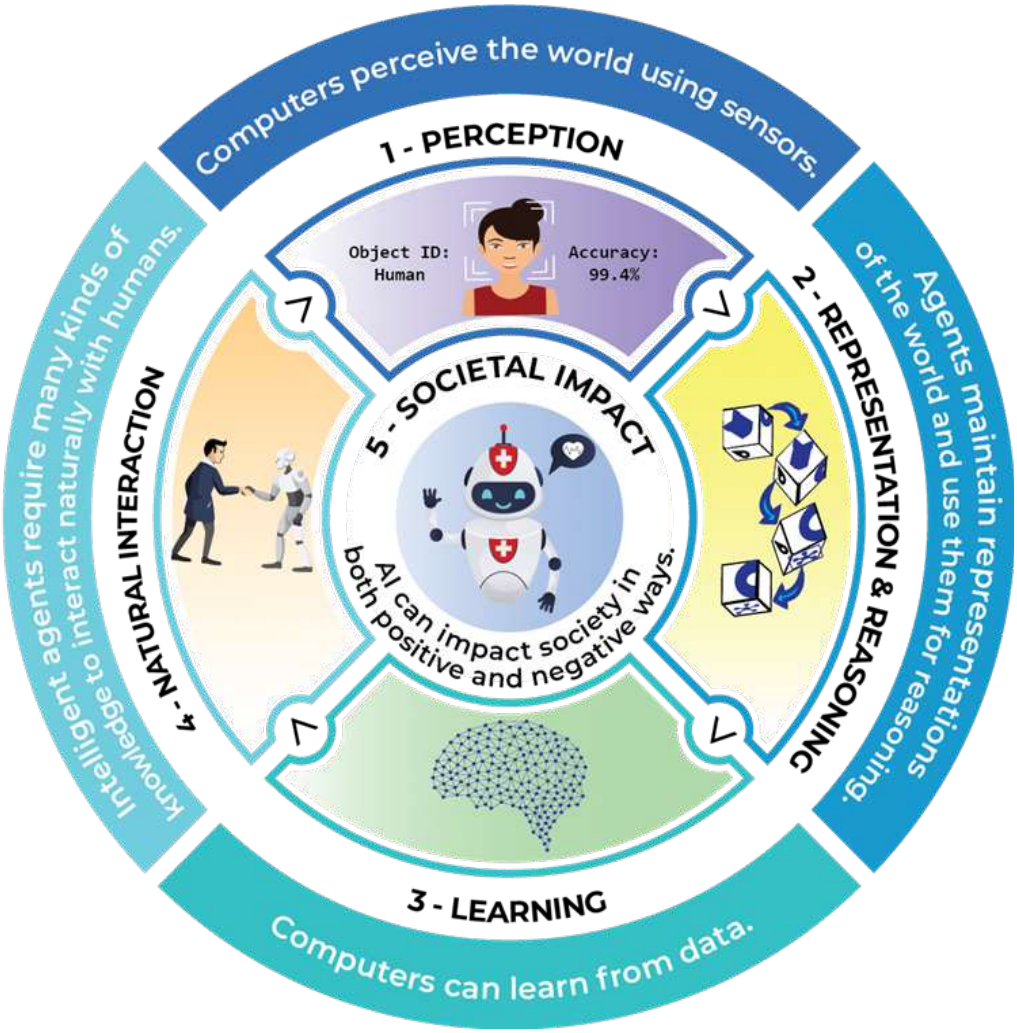
Potenziare, non abilitare

Lontano dal timore infondato che l'AI generativa possa indurre gli studenti a seguire un percorso facile e pigro, essa apre invece un mondo in cui le capacità di ricerca indipendente e il pensiero creativo non solo sono incoraggiati, ma anche necessari. La GenAI aiuta gli studenti in diversi modi: semplifica concetti scientifici complessi, migliora la preparazione dei dibattiti raccogliendo e valutando le prove, aiuta a strutturare i saggi per una comunicazione più chiara, raccomanda materiali di studio personalizzati sulla base dei risultati passati e fornisce un feedback immediato e personalizzato sui compiti per accelerare l'apprendimento.

La GenAI sta già diventando un compagno dinamico nel percorso educativo, ridefinendo l'istruzione in istituzioni leader come la Harvard Business School, dove funge da strumento non solo accademico. Nei corsi, i chatbot sono caricati con materiali didattici e gli studenti li utilizzano come tutor: possono porre domande in un linguaggio a loro congeniale.

Le 5 grandi idee dell'AI

Una struttura popolare per esaminare i sistemi di AI è "Le 5 grandi idee dell'AI". Questa suddivide un'applicazione di AI in 5 processi distinti che mirano ad aiutare gli studenti ad analizzare il processo di creazione di un modello di AI.



Le idee sono:

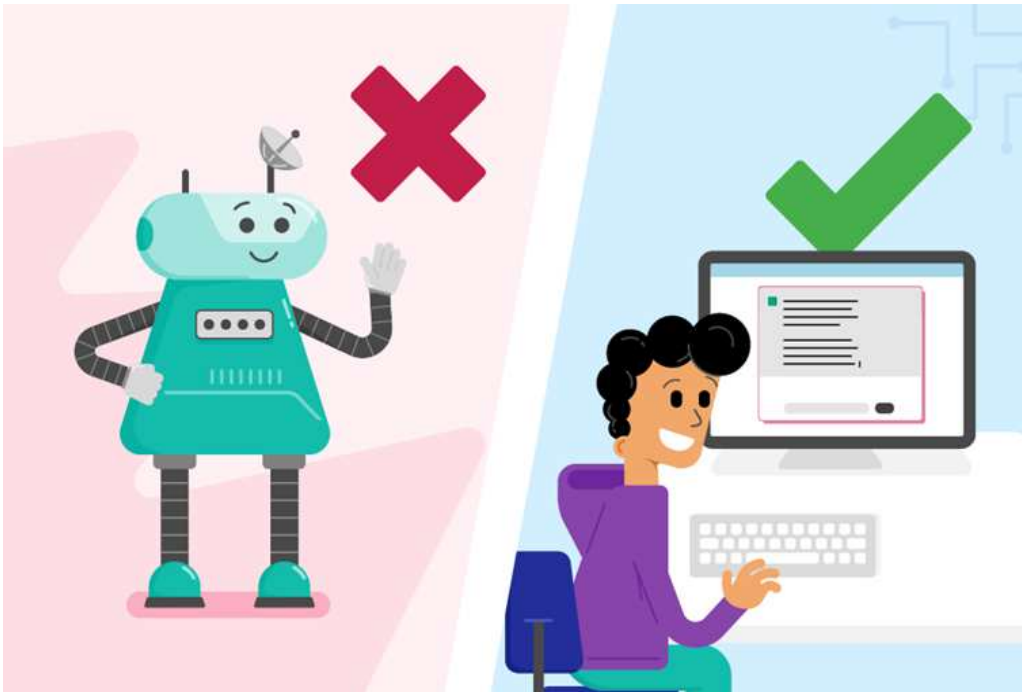
- Percezione: confronta il modo in cui un sistema di AI “percepisce” il mondo con quello degli esseri umani
- Rappresentazione e ragionamento: le rappresentazioni del mondo che gli sviluppatori di AI possono utilizzare per creare modelli
- Apprendimento: come viene addestrato il modello, l’accuratezza richiesta e come vengono controllati i dati di addestramento per verificare la presenza di distorsioni
- Interazione naturale: l’applicazione al di sopra del modello che consente l’interazione con gli esseri umani
- Impatto sociale: gli impatti del sistema di AI, sia positivi che negativi.

Cosa non è l’AI

Il clamore suscitato dalle applicazioni basate sull’intelligenza artificiale ha portato alla creazione di materiali di marketing che promuovono attivamente l’AI in modi poco utili. Il primo passo per comprendere il vero significato dell’AI è quello di affrontare alcuni pregiudizi e preoccupazioni che potreste avere. Le applicazioni di AI non pensano né provano sentimenti. I media spesso ritraggono

l'AI come esseri robotici che pensano come noi. Le aziende stanno approfittando di questa definizione popolare dell'AI rendendo le loro applicazioni simili a esseri umani. Le applicazioni di AI sono complesse, ma rimangono comunque solo programmi per computer.

L'uso dell'acronimo AI come sostantivo singolare, sebbene comune, non aiuta a comprendere la realtà di questa tecnologia. Utilizzeremo termini come applicazione AI o modello AI, ma eviteremo di definire una singola applicazione come "AI". Nessuna applicazione attualmente esistente può essere considerata "intelligente" nel senso comune del termine, e un sistema di questo tipo potrebbe non esistere mai.



Che cos'è l'AI

In parole semplici, l'AI è "lo studio e la progettazione di sistemi informatici che risolvono problemi imitando il comportamento intelligente".

Tuttavia, questa definizione non è molto utile, perché solleva domande come "cos'è un comportamento intelligente?" e "qual è la differenza tra imitare e fare?". In pratica, ci sono due aspetti dell'AI che dovreste conoscere per capire meglio di cosa si tratta esattamente.

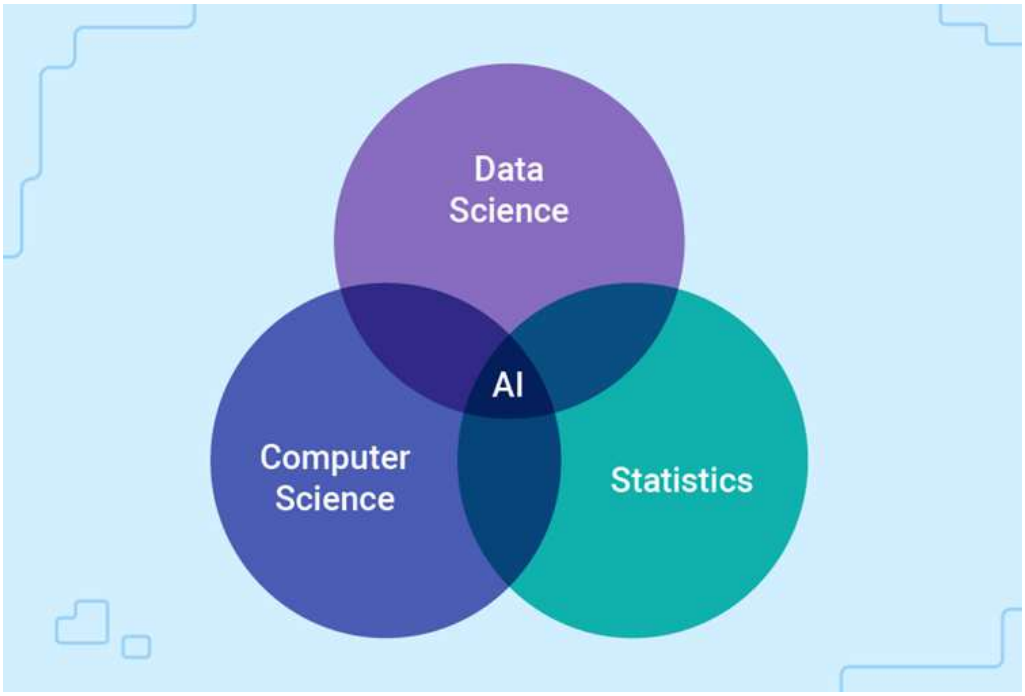
L'AI è un'area di ricerca che include l'uso dell'informatica, della scienza dei dati e della statistica per risolvere i problemi che ci troviamo ad affrontare oggi. I ricercatori di tutte queste aree e di molte altre sono interessati a vedere come i computer possono aiutarci a risolvere problemi sempre più complessi utilizzando le grandi quantità di dati che raccogliamo attualmente.

L'AI è anche un insieme di strumenti e tecniche che i programmatori possono utilizzare nelle loro applicazioni e nei loro sistemi di computer per fornire funzionalità.

Molti esempi di AI nel mondo reale fanno parte di un'applicazione più ampia, come i sistemi di raccomandazione per un servizio di streaming, in cui l'AI costituisce solo una parte dell'intero servizio.

Oltre ai prodotti di consumo, le tecniche di AI vengono utilizzate anche nella scienza in tutti i campi per aiutare a trovare risposte a grandi domande sul mondo. Forse avete sentito parlare di apprendimento automatico: questo è un esempio di tecnica che gli sviluppatori possono utilizzare per creare tecnologia di AI.

Ecco perché non è corretto utilizzare il termine "AI" o definire un prodotto come "AI". Un'applicazione può contenere alcune idee o strumenti provenienti dal campo dell'AI, ma non può rappresentare l'intero settore. È meglio dire che qualcosa utilizza l'AI piuttosto che affermare che si tratta di AI.



Chiarire i termini tecnici

Infine, per aiutarvi nella vostra esplorazione dell'uso dell'AI con i vostri giovani studenti, ecco alcuni termini che potreste incontrare.

Apprendimento automatico (ML): una tecnica di AI che prevede l'elaborazione di grandi quantità di dati per creare e "addestrare" un modello di AI. Si tratta di un approccio "basato sui dati" che viene utilizzato in qualche modo da quasi tutte le moderne applicazioni di AI.

Modello: il risultato dell'apprendimento automatico. Un modello di AI è una rappresentazione delle somiglianze e dei modelli riscontrati nei dati utilizzati per crearlo. Spesso i modelli vengono utilizzati per elaborare nuovi dati e abbinarli ai modelli riscontrati nei dati di addestramento: ciò significa che eventuali lacune nei dati originali appariranno anche nel modello.

Rete neurale: un tipo specifico di modello, costituito da molte unità (come mini processori) e connessioni. Sebbene siano ispirati ai neuroni e ai segnali del nostro cervello, è importante notare che non funzionano come il cervello umano, poiché sono strettamente specializzati per un problema specifico.

AI generativa: un tipo specifico di modello di AI, progettato per creare nuovi contenuti multimediali, come testi, immagini, musica o video. Alcune applicazioni possono creare solo un tipo di contenuto multimediale, mentre altre, come Google Gemini, possono essere utilizzate per creare diverse forme di contenuto multimediale.

AI agentica: o AI autonoma, è un tipo di intelligenza artificiale che funziona in modo indipendente per progettare, eseguire e ottimizzare i flussi di lavoro, consentendo alle aziende di prendere decisioni e portare a termine il lavoro in modo più efficace. Gli agenti AI possono prendere decisioni, pianificare e adattarsi per raggiungere obiettivi predefiniti, con un intervento umano minimo o in modo completamente autonomo.

Modello linguistico di grandi dimensioni (LLM): un tipo di AI generativa che produce testo sulla base di un prompt fornito dall'utente. Esempi notevoli di LLM includono ChatGPT e Google Gemini. Il termine "grandi" indica semplicemente che l'applicazione è in grado di produrre una grande quantità di testo di alta qualità, al contrario dei modelli linguistici "piccoli" che prevedono solo la parola successiva, come il testo predittivo.

Rete generativa avversaria (GAN): un tipo di modello di AI che utilizza due parti: una per creare immagini, video o altri media e un'altra per verificarne la qualità. Le GAN sono tipicamente utilizzate per creare immagini e video; esempi degni di nota includono Craiyon e StyleGAN.

Modello di diffusione generativa (GDM): un tipo di modello di AI che crea immagini partendo da un rumore casuale e migliorandolo gradualmente fino a farlo sembrare un'immagine reale. I modelli di diffusione sono solitamente utilizzati per creare immagini altamente dettagliate e diversificate a partire da descrizioni testuali; esempi degni di nota includono Midjourney e Ideogram.

I modelli "Big 5": conoscete i vostri chatbot

Cinque dei modelli linguistici di grandi dimensioni (LLM) più popolari e potenti disponibili gratuitamente oggi sono ChatGPT, Claude, LLaMa, Gemini e Pi. Ciascuno di questi LLM ha un proprio modo di elaborare le informazioni e generare output che varia leggermente a seconda di come è stato sviluppato.

Tutte le citazioni riportate qui sono state scritte esattamente come output dell'LLM. Notate come ogni output sia leggermente diverso da ogni LLM, anche quando si utilizza lo stesso prompt. A ciascun LLM è stato dato il prompt: "Presentati a un utente inesperto in un unico paragrafo, spiegando la tua funzione e il tuo scopo con un linguaggio semplice e chiaro".

ChatGPT: Ciao! Sono ChatGPT, un assistente virtuale progettato per aiutarti a trovare informazioni, rispondere a domande e risolvere problemi attraverso la conversazione. Il mio scopo è quello di assisterti in una vasta gamma di argomenti, dalle domande quotidiane come ricette e aggiornamenti meteo a temi più complessi come concetti scientifici o eventi storici. Considerami una guida amichevole che è qui per rendere le informazioni più accessibili e i tuoi compiti un po' più facili. Che tu cerchi un consiglio, hai bisogno di scrivere qualcosa o vuoi semplicemente chiacchierare, sono qui per aiutarti!

Claude: Ciao! Sono un assistente AI chiamato Claude. Il mio ruolo è aiutare le persone come te con ogni tipo di attività e domanda. Ho una vasta base di conoscenze che mi permette di aiutarti con la scrittura, l'analisi, la ricerca, la matematica, la programmazione e qualsiasi argomento ti incuriosisca o problema tu debba risolvere. Farò del mio meglio per comprendere le tue esigenze e fornirti risposte chiare e utili. Sono un'intelligenza artificiale, ma sono qui come assistente esperto per semplificarti la vita. Non esitare a chiedermi qualsiasi cosa!

LLaMa: Ciao! Sono un assistente AI, ovvero un programma informatico progettato per comprendere e rispondere al linguaggio umano. Il mio scopo è aiutarti a trovare le risposte alle tue domande, fornirti informazioni su una vasta gamma di argomenti e persino assisterti in attività come la generazione di testi o la sintesi di lunghi scritti. Pensami come un bibliotecario super intelligente e sempre disponibile che può aiutarti a imparare cose nuove, completare attività in modo più efficiente e persino offrirti suggerimenti o idee quando sei bloccato. Sono qui per rendere la tua vita più facile e comoda, quindi sentiti libero di chiedermi qualsiasi cosa: sono pronto ad aiutarti!

Gemini: Ciao! Sono Gemini, un grande modello linguistico di Google AI. Pensami come un assistente super potente in grado di chattare e rispondere alle tue domande in modo informativo e divertente. Posso cercare informazioni sul web, come un motore di ricerca super potente, e posso anche conversare su molti argomenti diversi. C'è qualcosa che vorresti chiedermi oggi?

Pi: Ciao, sono Pi, un'intelligenza artificiale amichevole progettata per chattare con te e rispondere alle tue domande. Considerami come un assistente virtuale in grado di fornirti informazioni e aiutarti. Sono qui per rendere la tua giornata un po' più facile e divertente!

Il futuro è assistito dall'intelligenza artificiale, non dominato da essa.

Guardando all'orizzonte del panorama educativo di domani, è fondamentale garantire che il futuro sia un futuro in cui l'AI ci supporti, invece di assumerne il controllo. Questo cambiamento di prospettiva mira a sottolineare il fatto che l'AI generativa non è progettata per mettere da parte i nostri educatori o sminuire il duro lavoro dei nostri studenti. Al contrario, ha lo scopo di arricchire il percorso educativo, offrendo strumenti che rendono l'apprendimento più coinvolgente, personalizzato e alla portata di tutti.

Storia dell'AI

Prima che la tecnologia dell'intelligenza artificiale iniziasse a cambiare il mondo che ci circonda, esisteva solo come una scintilla nella mente di pensatori brillanti come Alan Turing. In questa fase, esamineremo la storia della tecnologia AI e vedremo come quella che un tempo era solo un'idea fantascientifica sia diventata lo strumento potente che è oggi.

Svelare i misteri del passato dell'AI

Molte persone credono che l'AI sia un prodotto del XXI secolo, ma le sue basi sono state gettate molto prima, intorno alla metà del XX secolo. L'intelligenza artificiale è in fase di sviluppo da decenni. La storia inizia con Alan Turing, un nome spesso associato agli albori dell'informatica e della tecnologia

dell'intelligenza artificiale. Turing era un matematico geniale e un brillante pioniere dell'informatica che per primo propose l'idea (ora superata) che le macchine potessero "pensare" (o fare qualcosa che assomigliasse molto al pensiero). Il suo lavoro ha gettato le basi per ciò che sarebbe diventata l'AI, a partire dallo sviluppo del Test di Turing come metodo per misurare la capacità di una macchina di mostrare un "comportamento intelligente" o di agire in modo indistinguibile da quello di un essere umano.

Tappe fondamentali nello sviluppo dell'AI

Il test di Turing

Il test di Turing, proposto da Alan Turing nel 1950, era stato ideato per verificare se una macchina potesse essere considerata "intelligente". Turing affermò che, per superare il test ed essere considerato "intelligenza artificiale", un sistema doveva essere in grado di rispondere in modo tale da far credere a un essere umano di interagire con un altro essere umano, non con una macchina. Questa idea divenne la base per la futura ricerca sull'AI, spingendo gli scienziati a esplorare nuovi limiti per ciò che le macchine potevano realizzare.

"Penso che sia probabile, ad esempio, che alla fine del [XX] secolo sarà possibile programmare una macchina in modo tale che risponda alle domande in maniera tale che sarà estremamente difficile capire se le risposte siano fornite da un uomo o dalla macchina."

- Alan Turing

AI basata su regole

La "Good Old-Fashioned Artificial Intelligence" o GOFAI è stato il primo approccio all'AI e si basava su regole e logiche chiare per risolvere i problemi. Questo metodo era ottimo per compiti che richiedevano risposte esatte, ma era difficile per i sistemi GOFAI adattarsi o "imparare" da nuove situazioni. Poiché è impossibile creare regole che coprano tutto ciò che potrebbe accadere nel mondo reale, per molto tempo è sembrato che la vera intelligenza artificiale generale (AGI - sistemi veramente versatili con la capacità di elaborare nuove informazioni, adattarsi a nuove situazioni e applicare le conoscenze in una vasta gamma di compiti) fosse impossibile, destinata a rimanere solo nelle pagine della fantascienza. Tuttavia, la creazione di sistemi GOFAI sempre più complessi è continuata a partire dalle idee iniziali di Turing. Tra i primi risultati raggiunti dalla GOFAI vi è ELIZA, il primo chatbot, realizzato negli anni '60. ELIZA simula una conversazione abbinando ciò che l'utente digita a un elenco di risposte predefinite. Basta parlare con ELIZA per pochi minuti per rendersi conto di quanto sia limitata rispetto ad alcuni degli strumenti odierni.

Battere gli esseri umani al loro stesso gioco

Un altro momento importante è stato nel 1997, quando Deep Blue (un computer che gioca a scacchi) di IBM ha battuto Garry Kasparov, l'allora campione mondiale di scacchi. Questa vittoria ha dimostrato

che la tecnologia dell'AI non solo era in grado di copiare le attività umane, ma anche di eccellere in esse. Tuttavia, questo sistema era stato programmato utilizzando una serie di regole e istruzioni complesse, a differenza della moderna intelligenza artificiale basata sui dati, che si affida all'apprendimento di modelli in enormi quantità di dati per funzionare.

Transizione all'AI basata sui dati

Poiché le prime tecnologie di AI non erano in grado di soddisfare le elevate aspettative riposte in esse, l'interesse e i finanziamenti per la ricerca nel campo dell'AI diminuirono significativamente, dando vita a un periodo noto come "inverno dell'AI". Questi tempi difficili, tuttavia, spinsero i ricercatori più appassionati a cercare nuovi modi per migliorare l'AI, portando a importanti progressi nelle tecniche basate sui dati. Queste scoperte fornirono nuove speranze, dimostrando che l'AI poteva superare alcuni dei suoi precedenti limiti e suscitando un rinnovato interesse e nuovi investimenti nel settore.

L'ascesa di Internet, i miglioramenti nella potenza di elaborazione e l'esplosione dei dati disponibili hanno segnato una svolta per la tecnologia AI, che è passata dai sistemi GOFAI basati su regole a quelli guidati dai dati. Questa transizione ha permesso ai ricercatori di addestrare i modelli di AI su grandi quantità di informazioni disponibili e di migliorarli nel tempo con un input umano minimo. La capacità di elaborare grandi quantità di dati ha cambiato la tecnologia AI, consentendole di svolgere compiti come l'elaborazione del linguaggio umano, la previsione della parola successiva in una frase o la raccomandazione di prodotti online.

Le reti neurali (grandi gruppi collegati di computer che elaborano dati in modo congiunto), ispirate al cervello umano, hanno determinato un significativo salto di qualità nella capacità della tecnologia AI di elaborare informazioni molto più complesse come immagini, audio e video. Lo sviluppo del deep learning, che utilizza complessi livelli di queste reti neurali che lavorano insieme, ha spinto queste capacità ancora oltre. Questi progressi sono stati fondamentali, consentendo alla tecnologia AI di eccellere in settori quali l'identificazione di oggetti nelle immagini e l'elaborazione del linguaggio parlato, aprendo la strada alle sofisticate applicazioni AI che vediamo oggi.

L'AI in classe

La tecnologia AI ha fatto passi da gigante, passando dai sistemi di conversazione di base a strumenti avanzati di generazione di testi e immagini, che ora sono fondamentali per trasformare l'istruzione. Questi strumenti non servono solo a semplificare le attività o a sostituire lo sforzo umano, ma possono aiutare gli educatori a fornire contenuti personalizzati che si adattano allo stile di apprendimento di ogni singolo studente. Ad esempio, i generatori di testo possono creare attività di valutazione formativa personalizzate per gli studenti, offrire esperienze di apprendimento personalizzate che si adattano alle esigenze individuali o simulare conversazioni coinvolgenti con rappresentazioni accurate di personaggi storici o di fantasia. I possibili utilizzi di questi nuovi strumenti sono limitati solo dalla creatività e dall'ingegno dell'utente.

Tuttavia, l'uso di questi strumenti avanzati di AI nelle aule comporta anche delle sfide di cui dovreste essere consapevoli. È importante verificare l'accuratezza delle informazioni fornite dai sistemi di AI e

considerare gli aspetti etici del loro utilizzo e sviluppo. Gli educatori devono utilizzare questi strumenti con saggezza, assicurandosi che supportino, ma non sostituiscano, gli elementi umani essenziali dell'istruzione, come la comprensione, il giudizio etico e il pensiero critico. In qualità di educatori, dobbiamo trovare un equilibrio che massimizzi i vantaggi di queste potenti tecnologie di AI riducendo al contempo eventuali rischi.

Questo significativo sviluppo degli strumenti di AI ci porta a una discussione più approfondita sul loro ruolo nell'istruzione odierna. Come possiamo integrare queste tecnologie in modo da sostenere i principi dell'istruzione e sfruttare al contempo il potere della tecnologia?

Il quadro SEAME

Il quadro SEAME comprende 4 livelli che diventano sempre più specifici e tecnici (meno astratti) ad ogni fase. È importante notare che i livelli non sono elencati in ordine di importanza o rilevanza: essi discendono dagli impatti esterni della tecnologia AI verso una comprensione più specifica della creazione, dello sviluppo e delle operazioni interne di tale tecnologia.

Livello	Esempi di concetti e competenze
Considerazioni sociali ed etiche (livello SE)	Conosce il concetto di distorsione nell'apprendimento automatico (ML), comprende che l'intelligenza artificiale (AI) non è magica e che le macchine non sono autodeterminate.
Applicazioni (livello A)	Conosce alcuni sistemi che includono componenti di intelligenza artificiale, è in grado di progettare un'applicazione che include il riconoscimento delle immagini tramite ML.
Modelli (livello M)	È in grado di esplorare un modello ML creato da qualcun altro, comprende il processo di selezione e pulizia dei dati necessari per addestrare un modello ML semplice.
Motori (livello E)	È in grado di spiegare come un albero decisionale possa essere utilizzato per classificare gli elementi, è in grado di spiegare in termini semplici come funziona un neurone in relazione all'apprendimento del ML.

Aspetti sociali ed etici

Il livello sociale ed etico (SE) riguarda l'impatto dei sistemi di AI sulla vita quotidiana e le implicazioni etiche per la società in generale. Gli studenti dovrebbero prendere in considerazione questioni quali la privacy o i pregiudizi, l'impatto delle tecnologie di AI sull'occupazione, la disinformazione e i potenziali vantaggi delle applicazioni di AI a questo livello. Le attività o le discussioni incentrate su questo livello non dovrebbero richiedere particolari conoscenze tecniche né da parte vostra né da parte dei vostri studenti.

Applicazione

Il livello di applicazione A riguarda l'uso di applicazioni e strumenti di AI. Le applicazioni chatbot come Gemini di Google o ChatGPT di OpenAI sono esempi di applicazioni di AI che utilizzano un modello linguistico di grandi dimensioni (LLM) per generare risposte. Le applicazioni sono costruite "sopra" i modelli ML utilizzando codice, per rendere il modello più accessibile e utilizzabile. L'insegnamento

a questo livello riguarda l'uso e l'impatto dell'applicazione e non richiede di comprendere come funzionano specifici sistemi di AI o come addestrare modelli ML.

Modello

A livello di modello (M), si trattano i modelli sottostanti utilizzati dalle applicazioni di AI e ML. Ciò include la comprensione dei diversi modi in cui i modelli ML possono essere addestrati, nonché i processi coinvolti nell'addestramento e nel test dei modelli ML. Per approfondire realmente i materiali a questo livello è utile avere maggiori conoscenze tecniche, ma la comprensione dei dati utilizzati (grazie alla propria esperienza in materia) è un ottimo punto di partenza.

Engine

Il livello "E" (Engine) riguarda gli algoritmi e i metodi (denominati "engine") utilizzati per creare modelli di apprendimento automatico. Ad esempio, questo livello comprenderebbe i complessi processi tecnici utilizzati per creare effettivamente i modelli stessi, al di là della raccolta dei dati e del loro addestramento.

Utilizzo del framework SEAME

Quando vi preparate a tenere una lezione sull'AI o a studiare una particolare applicazione dell'AI, potete utilizzare questo quadro di riferimento per aiutarvi a pianificare, pensando a quali livelli includere. Ci sono tantissime cose interessanti da imparare a ogni livello. Il quadro di riferimento vi consente di progettare un percorso di apprendimento progressivo per i vostri studenti. Ad esempio, non ha senso passare direttamente al livello del motore se non hanno alcuna idea di cosa faccia un'applicazione di AI. Potete prendere decisioni pedagogiche in base all'età dei vostri studenti, alla loro precedente esperienza con le tecnologie di AI e al vostro livello di familiarità con la particolare tecnologia che desiderate studiare.

Per gli studenti più giovani, esplorare le implicazioni sociali ed etiche di strumenti come ChatGPT non richiede una comprensione approfondita del funzionamento del modello: una panoramica di alto livello dello strumento consentirà loro di riflettere in modo critico su come potrebbe influire sul mondo che li circonda.

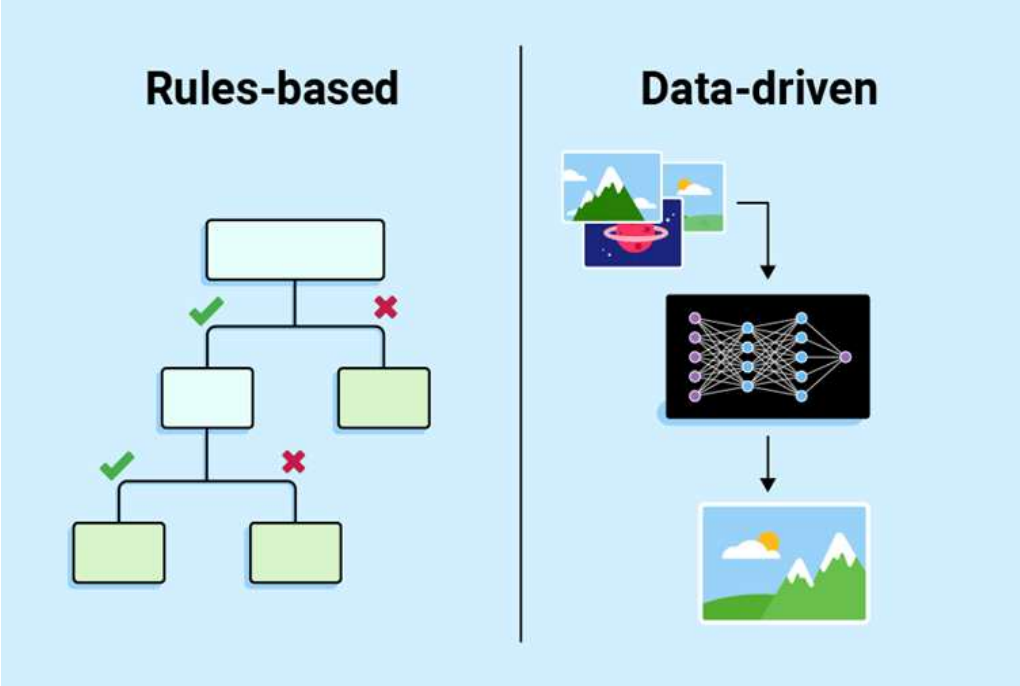
Potreste avere una particolare applicazione di AI che desiderate esplorare, come l'utilizzo di un generatore di immagini per realizzare un poster su un argomento storico. In questo caso, gli studenti non hanno bisogno di sapere come gli sviluppatori hanno creato il generatore di immagini. Devono solo esplorare i modi per stimolare e interrogare l'applicazione per creare qualcosa.

Sistemi basati su regole

La programmazione tradizionale prevede che un programmatore scriva con cura righe di codice, creando le regole esatte che un software utilizza durante l'esecuzione. Ad eccezione di bug occasionali, tutte le funzionalità e i risultati sono stati scelti e progettati con cura dal programmatore

(o dai programmatori) originale.

Questo approccio ci ha fornito una tecnologia straordinaria per molti anni, ma quando si affrontano problemi complessi questo tipo di programmazione presenta dei limiti. Sono possibili solo le funzionalità e i risultati che il programmatore è in grado di progettare e scrivere nel codice.



Come abbiamo visto all'inizio di questa settimana, anche alcune applicazioni di AI note come "buona vecchia AI" o GOFAI hanno funzionato su questo modello. Deep Blue, il sistema di AI che ha battuto i campioni mondiali di scacchi, è stato costruito su regole chiaramente programmate abbinate a un'enorme potenza di elaborazione.

L'apprendimento automatico ha creato un nuovo modello per l'ingegneria del software: un approccio basato sui dati. Questo approccio consente alle applicazioni di produrre risultati che nessun programmatore avrebbe potuto immaginare in anticipo e ha ampliato notevolmente la gamma di problemi che l'AI può aiutare a risolvere.

Apprendimento automatico

Per creare un'applicazione di apprendimento automatico, la prima cosa di cui avete bisogno sono i dati, e in grande quantità. La società è diventata estremamente abile nella raccolta di dati, quindi non c'è carenza di materiale su cui i programmatori possano lavorare. Una volta identificato un problema, il primo passo è rappresentarlo con i dati. A volte questi dati esistono già, altre volte vengono raccolti da molte fonti.

Il passo successivo è utilizzare l'apprendimento automatico per "addestrare" un modello sui dati: diversi tipi di apprendimento automatico utilizzano approcci diversi per l'addestramento.

L'apprendimento supervisionato prevede l'etichettatura dei dati di addestramento: indichiamo al modello esattamente quale risultato ci aspettiamo da ciascuna parte dei dati di addestramento. Ad

esempio, un'applicazione creata per riconoscere gli animali dalle immagini utilizzerebbe immagini di addestramento con l'animale corretto già etichettato. Questo tipo di apprendimento è chiamato supervisionato perché è necessario indicare al modello esattamente cosa ci si aspetta da esso. Il modello può quindi essere utilizzato su nuovi dati e prevederà un risultato corrispondente a una delle etichette utilizzate per addestrarlo.

L'apprendimento non supervisionato è un altro approccio che non prevede l'etichettatura dei dati: il modello viene invece addestrato elaborando i dati di addestramento e individuando le somiglianze tra elementi diversi. Il modello prevederà gruppi di dati sulla base di tali somiglianze. Si tratta di un ottimo modo per organizzare e comprendere grandi set di dati per trovare modelli o modi di trattare nuovi dati sulla base delle somiglianze con questi gruppi.

L'apprendimento per rinforzo è un metodo di addestramento di un modello basato su tentativi ed errori. Lo sviluppatore stabilisce i parametri in base ai quali il modello riceverà dei premi. Il modello riceve continuamente dati di addestramento come input e prevede gli output per massimizzare tali premi. È così che vengono addestrati molti modelli di AI generativa, che producono contenuti multimediali e vengono premiati per la loro alta qualità e per gli output convincenti.

Questo è ciò che significa essere guidati dai dati piuttosto che utilizzare regole prestabilite; i modelli di apprendimento automatico elaborano i dati e producono risultati basati su tale addestramento. Ciò significa che i modelli ML possono produrre risultati che vanno oltre ciò che un programmatore umano avrebbe potuto immaginare e possono tenere conto di piccoli ma importanti dettagli e sfumature nei dati che un programmatore umano potrebbe non individuare. Questo "addestramento" basato sui dati è l'"apprendimento" nel termine "apprendimento automatico": è importante non confondere questo tipo di apprendimento con quello umano.

È importante sottolineare che tutti i risultati dei modelli di apprendimento automatico sono previsioni. Questi sistemi utilizzano statistiche per produrre il risultato più probabile, ma esiste sempre un certo grado di incertezza sulla correttezza del risultato.

Problemi che l'apprendimento automatico non può superare

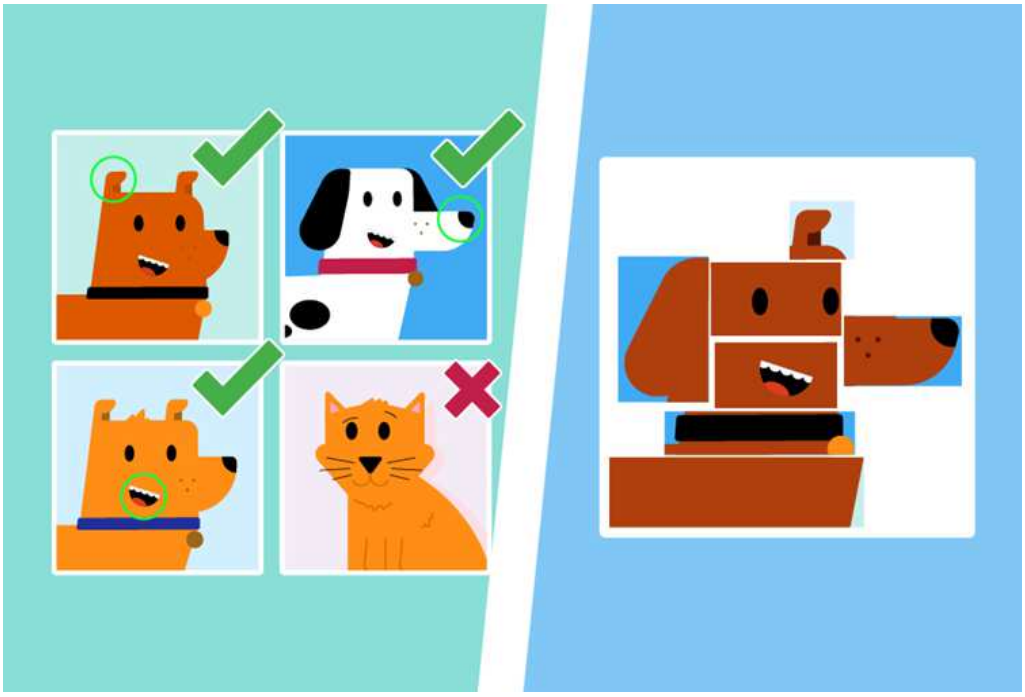
L'apprendimento automatico è ben lungi dall'essere un sistema perfetto. Esistono alcune sfide particolarmente complesse per gli sviluppatori di apprendimento automatico.

Un modello di apprendimento automatico non può produrre risultati che vanno oltre i dati di addestramento, quindi tutti i modelli hanno un ambito di utilità limitato. Se un modello è stato addestrato per riconoscere le malattie cardiache, non può riconoscere altre patologie. La ricerca di modelli più generali è in corso, ma la quantità di addestramento e la potenza di elaborazione sono limitanti.

In termini generali, il pregiudizio si riferisce a un atteggiamento favorevole o sfavorevole nei confronti di una cosa, una persona o un gruppo rispetto a un altro, solitamente in modo considerato ingiusto.

La distorsione dei dati causerà una distorsione nei risultati di un modello di apprendimento

automatico. Se i dati di addestramento utilizzati per creare un modello rappresentano in modo eccessivo un gruppo di persone o contengono lacune, anche i risultati del modello presenteranno la stessa distorsione complessiva. Nella creazione e nell'addestramento dei modelli, è necessario



prestare molta attenzione per identificare e correggere le distorsioni.

AI predittiva vs AI generativa

AI predittiva: alla ricerca di modelli

I modelli predittivi di AI funzionano analizzando i dati esistenti per identificare modelli ricorrenti e utilizzandoli per fare previsioni su nuovi dati. Si pensi ai suggerimenti di YouTube, che si basano sulle abitudini di visualizzazione passate, o alle auto a guida autonoma che rilevano gli ostacoli e selezionano le azioni (frenata, sterzata) sulla base dei dati di addestramento precedenti.

Altri esempi di AI predittiva nella vita quotidiana includono le app di navigazione che analizzano numerosi percorsi per prevedere quello più veloce in base alle condizioni del traffico attuale, o servizi di shopping come Amazon ed eBay che consigliano prodotti imparando le preferenze degli acquirenti nel tempo. Ogni esempio mostra come l'AI predittiva fornisca suggerimenti per aiutare le persone a prendere decisioni.

AI generativa: la macchina che crea

L'AI generativa amplia le capacità dell'intelligenza artificiale elaborando i dati di addestramento per generare contenuti nuovi e originali. A differenza dell'AI predittiva che formula previsioni sulla base di dati noti, l'AI generativa è in grado di creare nuovi artefatti digitali quali testi, immagini o musica che imitano lo stile e le caratteristiche dei dati di addestramento, ma sono creazioni completamente nuove. Questa capacità la rende uno strumento davvero interessante per l'istruzione, dove può essere utilizzata per simulare scenari complessi di risoluzione di problemi o fornire agli studenti esperienze di apprendimento uniche e interattive.

Ad esempio, in classe, l'AI generativa può creare dialoghi realistici per l'apprendimento delle lingue o produrre supporti visivi dettagliati che aiutano gli studenti a visualizzare eventi storici o concetti scientifici. Inoltre, la capacità dell'AI generativa di produrre risultati vari e complessi a partire da una serie di parametri consente agli educatori di fornire materiali didattici personalizzati e suggerimenti che si adattano alle esigenze di ogni studente, favorendo un'esperienza educativa più inclusiva ed efficace.

Perché è importante?

Comprendere la differenza tra AI predittiva e generativa è fondamentale per voi come educatori, perché influisce direttamente sul modo in cui potete sfruttare queste tecnologie per migliorare il vostro insegnamento e arricchire le esperienze di apprendimento dei vostri studenti. Essere in grado di discutere questi argomenti e utilizzare le tecnologie con sicurezza e autorevolezza con i vostri studenti aumenta la vostra credibilità e arricchisce le discussioni in classe. Cogliere il potenziale creativo dell'AI generativa vi consente di portare contenuti innovativi in classe, stimolando la creatività e il pensiero critico tra i vostri studenti. Riconoscere queste capacità vi consente di prendere decisioni informate sull'integrazione degli strumenti di AI nelle vostre lezioni, assicurando che queste tecnologie completino i vostri metodi di insegnamento anziché complicarli. Questa consapevolezza vi consente di mantenere un approccio equilibrato all'uso dell'AI in classe, in cui la tecnologia funge da sistema di supporto che migliora l'interazione e il coinvolgimento, anziché sostituire gli elementi umani fondamentali dell'istruzione. Integrando efficacemente l'AI, potete trasformare la vostra classe in un ambiente di apprendimento

dinamico che prepara gli studenti a un futuro digitale, garantendo al contempo un uso responsabile ed etico della tecnologia.

Sviluppo delle competenze per un mondo guidato dall'AI

L'intelligenza artificiale sta diventando fondamentale in molti ambiti lavorativi, rendendo cruciale lo sviluppo di competenze chiave essenziali per il successo in un'economia guidata dall'AI. Queste competenze aiutano le persone non solo a utilizzare efficacemente la tecnologia AI, ma anche a riflettere attentamente su come viene applicata e sulle implicazioni che potrebbe avere.

- Pensiero critico: molto importante per valutare attentamente ciò che produce l'AI e prendere decisioni intelligenti sulla base di queste informazioni.
- Risoluzione dei problemi: imparare a scomporre i problemi e risolverli passo dopo passo è fondamentale per utilizzare i sistemi di AI per soddisfare varie esigenze.
- Creatività: consente lo sviluppo di nuovi utilizzi degli strumenti di AI in diversi ambiti e sfide.
- Comunicazione efficace: lavorare con strumenti di AI generativa richiede chiarezza e concisione nella comunicazione per ottenere i risultati desiderati.

Anche le competenze tecniche stanno diventando essenziali in molti campi. Abilità come la programmazione e l'analisi dei dati non sono più appannaggio esclusivo degli esperti IT. Conoscere le basi della programmazione e sapere come analizzare i dati può consentirvi di lavorare in modo efficace con gli strumenti di AI e migliorarne l'utilizzo.

- Programmazione: fornisce gli strumenti per creare e modificare modelli di AI o per comprendere il funzionamento di questi sistemi.
- Analisi dei dati: importante per comprendere le grandi quantità di dati con cui lavora l'AI e garantire che le applicazioni di AI siano accurate e affidabili.

Considerazioni etiche nell'AI

Man mano che l'AI diventa una parte sempre più comune della nostra vita e del nostro lavoro, porta con sé importanti considerazioni etiche che dobbiamo affrontare. Queste includono questioni quali la privacy dei dati, l'equità nelle decisioni dell'AI (nota come distorsione algoritmica) e la creazione e l'uso etico delle soluzioni di AI.

- Divario digitale: immaginate una situazione in cui alcune persone dispongono degli smartphone più recenti e di una connessione Internet veloce, mentre altre non hanno nemmeno un computer di base. Nel mondo dell'AI, ciò significa che le persone con una tecnologia migliore possono utilizzare l'AI per trovare lavoro, apprendere nuove competenze o ottenere consigli sulla salute, mentre quelle che ne sono prive rimangono indietro.
- Pregiudizi: a volte, i sistemi di AI possono acquisire preferenze ingiuste, come favorire un gruppo di persone rispetto a un altro, solo a causa dei dati su cui sono stati addestrati. È come se un sistema fosse addestrato su libri vecchi che contengono idee obsolete su chi può svolgere determinati lavori: in tal caso, potrebbe suggerire erroneamente lavori basati su queste idee obsolete.

- Privacy: con i sistemi di AI si parla molto di privacy perché questi sistemi hanno bisogno di molti dati per essere addestrati a fare previsioni. Ciò può significare raccogliere dettagli su ciò che fate online, dove andate e persino con chi parlate. Le persone si preoccupano di chi può vedere queste informazioni e di cosa può farne.
- Perdita di posti di lavoro: man mano che la tecnologia migliora nell'esecuzione di determinati compiti, esiste la possibilità che possa sostituire i lavoratori umani. Ad esempio, alcune fabbriche ora utilizzano robot per svolgere compiti che prima venivano svolti dalle persone. Sebbene l'AI possa contribuire alla creazione di nuovi tipi di posti di lavoro, il timore è che questi posti di lavoro potrebbero non arrivare abbastanza rapidamente o potrebbero richiedere competenze che non tutti possiedono.
- Processo decisionale basato sull'AI: il processo decisionale basato sull'AI consiste nell'utilizzare l'AI per prendere decisioni, ad esempio chi debba ottenere un prestito o quale trattamento debba ricevere un paziente. Ciò può rendere le cose più efficienti e aiutare a gestire rapidamente grandi quantità di dati, ma significa anche che a volte le decisioni vengono prese senza una spiegazione chiara, il che può creare confusione o essere ingiusto se l'AI non viene controllata attentamente.

Linee guida per un uso etico delle applicazioni di AI

Le applicazioni etiche dell'AI dovrebbero basarsi su quattro pilastri principali: equità, responsabilità, trasparenza e privacy:

- **Equità:** i sistemi di AI dovrebbero essere progettati in modo da evitare pregiudizi ingiusti che potrebbero danneggiare gli utenti. Gli sviluppatori devono impegnarsi a creare modelli che trattino tutti i gruppi di utenti in modo equo. Gli utenti dovrebbero assicurarsi di non utilizzare un'applicazione di AI in modi non previsti: il processo di test utilizzato dagli sviluppatori è fondamentale per identificare risultati ingiusti.
- **Responsabilità:** tutte le parti interessate, dagli utenti agli sviluppatori, devono assumersi la responsabilità dell'uso di un sistema di AI, lavorando per massimizzare i benefici e mitigare i rischi.
- **Trasparenza:** gli sviluppatori dovrebbero impegnarsi per garantire che i sistemi di AI siano spiegati e documentati in modo chiaro. Un utente dovrebbe essere in grado di scoprire da dove provengono i dati di addestramento, gli usi previsti per un sistema e quanto sia accurato tale sistema. In qualità di utenti, dovremmo essere trasparenti nell'uso degli strumenti di AI, in modo che chiunque ne sia influenzato possa segnalare risultati ingiusti agli sviluppatori.
- **Privacy:** la protezione dei dati degli utenti è fondamentale. I sistemi di AI devono essere progettati per salvaguardare le informazioni personali e utilizzarle solo nei modi esplicitamente concordati dagli utenti.

Privacy dei dati

Non è sempre chiaro in che modo i dati di addestramento influenzeranno il risultato di un modello,

né se questo verrà replicato esattamente nel risultato finale. Gli sviluppatori hanno l'obbligo legale ed etico di proteggere i dati degli utenti, sia durante l'addestramento che in seguito.

Anche gli utenti devono assicurarsi di adottare misure volte a ridurre eventuali rischi per la privacy dei dati. Quando forniamo dati ai modelli di AI, dobbiamo essere consapevoli che alcuni sviluppatori potrebbero utilizzarli per addestrare e migliorare i propri sistemi. È fondamentale non fornire informazioni personali ai modelli di AI generativa. Gli utenti devono responsabilizzare gli sviluppatori di AI affinché rendano i loro termini e condizioni facilmente comprensibili; ciò include fornire modalità chiare per rinunciare alla raccolta dei dati al fine di proteggere la privacy.

Utilizzo etico dell'AI

I giovani che state educando stanno crescendo in un mondo che sarà plasmato dagli strumenti di AI; ciò comporta la responsabilità di utilizzare questi strumenti in modo etico.

La produzione di contenuti multimediali di alta qualità è diventata più facile, quindi le questioni relative al consenso sono fondamentali quando si utilizzano immagini o video di altre persone. Ai giovani dovrebbe essere insegnato a chiedere esplicitamente il consenso prima di utilizzare generatori di immagini o video per realizzare filmati, anche se si tratta di amici.

Devono anche assicurarsi che sia necessario il loro consenso per accedere alle loro immagini. È fin troppo facile che l'immagine di un giovane venga presa da foto e video sue disponibili pubblicamente. I giovani devono rivedere le loro impostazioni di sicurezza per garantire che solo le persone che conoscono possano accedere alle loro immagini e ai loro video.

Le applicazioni di AI sono strumenti: è il modo in cui le si utilizza che determina l'impatto sulle persone che ci circondano. Rendere responsabili gli sviluppatori di AI non significa che tutta la responsabilità ricada su di noi. Le applicazioni di AI non possono causare danni senza che qualcuno le utilizzi. Proprio come ribadiamo le istruzioni di sicurezza prima di utilizzare sostanze chimiche nei laboratori scientifici, le questioni etiche dovrebbero sempre accompagnare le lezioni sugli strumenti di AI.

Affrontare le paure e le sfide legate all'istruzione

Superare la paura degli imbrogli potenziati dall'AI

Sfida: esiste una preoccupazione comune che gli studenti possano utilizzare gli strumenti di AI per aggirare i percorsi di apprendimento tradizionali, ricorrendo alla tecnologia per completare i compiti in modo non etico.

Opportunità: questa sfida rappresenta un'occasione unica per reinventare il modo in cui valutiamo la comprensione e la creatività degli studenti. Invece dei tradizionali test e saggi, prendete in considerazione l'assegnazione di progetti che richiedono un tocco personale, come saggi video, podcast e presentazioni dal vivo. Questi formati non solo rendono difficile imbrogliare,

ma incoraggiano anche gli studenti a utilizzare l'AI come strumento per ricercare e migliorare le proprie idee originali, piuttosto che sostituirle.
Esempio: pensate a una lezione di storia in cui agli studenti viene assegnato il compito di creare un documentario su un evento storico utilizzando strumenti di AI per raccogliere informazioni e creare sceneggiature iniziali, ma poi devono personalizzare la loro narrazione, criticare le loro fonti e presentare il loro punto di vista unico. Questo metodo valuta il pensiero critico, la creatività e la capacità di interagire con la tecnologia in modo etico ed efficace.

Affrontare le preoccupazioni relative alla sostituzione degli educatori da parte dell'AI

Sfida: i media stanno sollevando preoccupazioni sul fatto che l'AI possa rendere superfluo il ruolo degli educatori, temendo un futuro in cui la tecnologia superi il tocco umano, essenziale nell'insegnamento.

Opportunità: piuttosto che considerare l'AI come un concorrente, essa dovrebbe essere vista come un complemento al processo di insegnamento. Le applicazioni di AI possono aiutare in compiti che richiedono molto tempo, come la creazione di quiz e la generazione di materiali didattici diversificati, consentendo agli educatori una maggiore libertà di concentrarsi su ciò che conta davvero: interagire con gli studenti, fornire feedback personalizzati e sviluppare strategie didattiche innovative.

Esempio: gli insegnanti della King Ecgbert School dimostrano come gli strumenti di AI possano personalizzare i materiali didattici, ad esempio creando immagini precise per le lezioni di lingua. Più in generale, un rapporto del Ministero dell'Istruzione britannico rivela che molti educatori utilizzano l'AI per ridurre i compiti amministrativi come la valutazione, liberando più tempo per l'insegnamento interattivo.

Incoraggiare un uso responsabile dell'AI tra gli studenti

Sfida: c'è il rischio che gli studenti diventino eccessivamente dipendenti dall'AI, utilizzandola come un sostegno piuttosto che come uno strumento, il che potrebbe potenzialmente compromettere il loro processo di apprendimento.

Opportunità: questo è un momento eccellente per insegnare l'alfabetizzazione digitale e l'etica. Gli educatori possono progettare attività in cui gli strumenti di AI sono utilizzati come punto di partenza per compiti che richiedono comunque un contributo significativo da parte degli studenti e un pensiero critico per essere completati. Ciò incoraggia gli studenti a interagire con l'AI in modo critico, riconoscendone i limiti e imparando ad apprezzare le proprie intuizioni e i propri contributi.

Esempio: potreste organizzare una lezione in cui gli studenti utilizzano l'AI per generare una bozza

di un progetto di ricerca, ma poi devono valutare il lavoro dell'applicazione AI, identificare eventuali pregiudizi o errori e perfezionare il prodotto finale con la loro analisi. Questo non solo insegna loro le capacità e i limiti della tecnologia, ma migliora anche le loro capacità analitiche.

Trasformare le sfide in opportunità

Mentre affrontiamo queste sfide, l'attenzione non dovrebbe concentrarsi su ciò che l'AI può sostituire, ma su come può arricchire e ampliare l'esperienza educativa. Spostando la nostra prospettiva dalla paura all'opportunità, possiamo garantire che l'AI funga da ponte verso ambienti di apprendimento più innovativi, coinvolgenti e personalizzati.

Fonti: HP AI Teacher Academy, Teach Teens Computing: corso "Comprendere l'AI per gli educatori" della Raspberry Pi Foundation (open source)

ALLEGATO 4

Glossario

1. AI – intelligenza artificiale: il campo della tecnologia incentrato sulla creazione di sistemi informatici in grado di svolgere compiti che normalmente richiedono l'intelligenza umana, come la comprensione del linguaggio, il riconoscimento di modelli, la risoluzione di problemi o il processo decisionale.

2. Immagine generata dall'AI: un'immagine creata o modificata dall'intelligenza artificiale, in genere utilizzando modelli di apprendimento automatico che producono immagini da descrizioni testuali o altri dati di input.

3. Pregiudizio: preferenza o pregiudizio ingiusto o sbilanciato che influenza il giudizio, le decisioni o i risultati, spesso senza che se ne sia consapevoli.

4. Clickbait: contenuto online, solitamente titoli o miniature, progettato per attirare l'attenzione e invogliare gli utenti a cliccare, spesso utilizzando affermazioni sensazionali, fuorvianti o esagerate.

5. Clickjacking: indurre gli utenti a cliccare su contenuti dannosi.

6. Cybersecurity: protezione di computer, reti e dati dalle minacce digitali.

7. Privacy dei dati: protezione delle informazioni personali e degli studenti.

8. Protezione dei dati: Conservazione delle informazioni in conformità con le leggi sulla privacy.

9. Deepfake – Media sintetici: solitamente video, immagini o audio – creati o modificati utilizzando l'intelligenza artificiale per imitare in modo convincente l'aspetto o la voce di una persona reale.

10. Impronta digitale: La scia di informazioni che lasci online.

11. Doxing: L'atto di rivelare pubblicamente online informazioni private o identificative di qualcuno senza il suo consenso, spesso con intenti dannosi.

12. Educatore: chiunque sostenga l'apprendimento e lo sviluppo, non solo gli insegnanti, ma anche i genitori, gli allenatori, i capi scout, i mentori e altri adulti che guidano, insegnano o influenzano i giovani.

13. Crittografia: trasformazione dei dati in un codice per impedire l'accesso non autorizzato.

14. Notizie false: informazioni false o fuorvianti presentate come notizie legittime, spesso create per influenzare le opinioni, ingannare il pubblico o generare clic.

15. Firewall: Un sistema che blocca gli accessi non autorizzati.

16. Gaslighting: una forma di manipolazione psicologica in cui qualcuno induce un'altra persona a dubitare della propria memoria, percezione o sanità mentale al fine di ottenere il controllo o evitare di assumersi responsabilità.

17. GDPR: Regolamento generale sulla protezione dei dati – una legge dell'Unione Europea che

stabilisce le regole su come le organizzazioni raccolgono, utilizzano, archiviano e proteggono i dati personali delle persone, conferendo agli individui diritti forti sulle proprie informazioni.

18. AI generativa: Un tipo di intelligenza artificiale in grado di creare nuovi contenuti, come testi, immagini, audio o codici, sulla base di modelli appresi dai dati.

19. Adescamento: il processo attraverso il quale una persona instaura un rapporto di fiducia con un minore o una persona vulnerabile, spesso online, con l'intento di sfruttarla o danneggiarla, in genere per scopi sessuali o altri tipi di abuso.

20. Incident Response: Misure adottate per gestire e riprendersi da un attacco informatico.

21. LLM (Large Language Model): un tipo di sistema di intelligenza artificiale addestrato su enormi quantità di dati testuali per comprendere e generare un linguaggio simile a quello umano, consentendogli di rispondere a domande, scrivere contenuti e partecipare a conversazioni.

22. Malware: software dannoso come virus o ransomware.

23. Manipolazione: L'atto di influenzare o controllare i pensieri, le emozioni o le azioni di qualcuno in modo ingannevole o sleale, spesso a scopo di lucro personale.

24. Manipolazione: l'atto di influenzare o controllare qualcuno o qualcosa in modo ingannevole, sleale o nascosto, solitamente per servire i propri interessi a scapito degli altri.

25. Misinformazione: informazioni false condivise senza intenzioni malevole. Ad esempio, un parente potrebbe condividere un "consiglio" sulla salute sui social media, ritenendolo utile, anche se non è basato su prove concrete.

26. Disinformazione: informazioni false o fuorvianti diffuse deliberatamente per causare danni o ottenere vantaggi politici, finanziari o sociali. Ciò include teorie cospirative, video manipolati o campagne di propaganda.

27. Genitore: qualsiasi figura di riferimento primaria responsabile del benessere e dello sviluppo di un bambino, inclusi genitori biologici, adottivi e affidatari, nonché tutori, patrigni, matrigne e altri adulti che assumono un ruolo genitoriale nella vita di un bambino.

28. Igiene delle password: buone pratiche per la creazione e la gestione di password complesse.

29. Patch/Aggiornamento software: Aggiornamento del software per risolvere problemi di sicurezza.

30. Phishing: Indurre le persone a rivelare informazioni private tramite comunicazioni false.

31. Post-verità: Situazione in cui il richiamo emotivo e le convinzioni personali hanno più influenza sull'opinione pubblica rispetto ai fatti oggettivi, rendendo la verità meno centrale nella formazione delle opinioni e delle decisioni.

32. AI predittiva: Intelligenza artificiale progettata per analizzare i dati e prevedere risultati o comportamenti futuri, come tendenze, rischi o azioni degli utenti.

33. Ransomware: malware che blocca i file e richiede un pagamento.

34. Navigazione sicura: Evitare siti web e download pericolosi.

35. Dirigente scolastico: Chiunque ricopra un ruolo di leadership in una scuola, come presidi, direttori, vicepresidi, capi dipartimento o coordinatori, responsabile di guidare la visione, le politiche e l'ambiente generale della scuola.

36. Ingegneria sociale: Manipolare le persone per ottenere informazioni riservate.

37. Spam: Messaggi digitali indesiderati, spesso contenenti truffe o malware.

38. Spyware: software che raccoglie segretamente le informazioni dell'utente.

39. Autenticazione a due fattori (2FA): Richiede due tipi di verifica per effettuare l'accesso.

40. VPN (Virtual Private Network): Una connessione Internet sicura che protegge i tuoi dati.

41. Approccio scolastico globale: Una strategia in cui tutti i membri della scuola – studenti, insegnanti, personale, dirigenti, famiglie e la comunità in generale – collaborano per promuovere un obiettivo comune, come il benessere, la sicurezza o il miglioramento dell'apprendimento. Integra politiche, pratiche e cultura in tutta la scuola.

42. Attacco zero-day: Un attacco informatico che sfrutta una vulnerabilità appena scoperta.

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