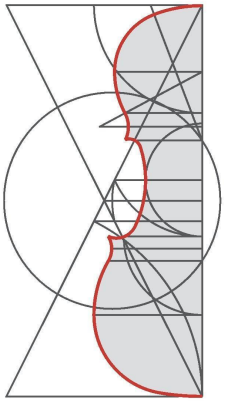


ISTITUTO DI ISTRUZIONE SUPERIORE
ANTONIO STRADIVARI
CREMONA

ISTITUTO DI ISTRUZIONE SUPERIORE "ANTONIO STRADIVARI" – CREMONA

Scuola Internazionale di Liuteria · Liceo Musicale · Liceo Artistico · Istituto Tecnico e Professionale per la Moda e l'Arredo

DOCUMENTO DI ePOLICY

Linee guida per l'uso consapevole e sicuro delle tecnologie digitali

Anno scolastico 2025/2026

c.f. – p.i. 80004640191 · cod. min. CRIS00800D

Indice

Premessa e riferimenti normativi

La redazione di una ePolicy per la scuola secondaria di secondo grado non è solo un adempimento formale, ma un documento strategico che integra diverse direttrici normative. Negli ultimi anni (2024–2026) il quadro si è evoluto significativamente, spostando l'accento sulla responsabilità dello studente e sull'uso consapevole dei dispositivi.

L'Istituto ha già approvato regolamenti riguardanti l'uso consapevole e responsabile delle tecnologie digitali, la sicurezza online e la protezione dei dati personali, la prevenzione e il contrasto al cyberbullismo, la netiquette e i comportamenti corretti in rete, l'uso appropriato dei dispositivi a scuola, l'educazione alla cittadinanza digitale e alla gestione dell'identità e della reputazione online, l'uso etico dell'intelligenza artificiale, il contrasto alla disinformazione, la promozione del benessere digitale, l'inclusione e l'accessibilità, la formazione della comunità scolastica e la definizione di responsabilità e sanzioni in caso di utilizzo improprio delle tecnologie.

I regolamenti sono consultabili sul sito web della scuola: Carte della scuola – istitutostradivari.edu.it

Di seguito i principali riferimenti normativi suddivisi per aree tematiche.

Cyberbullismo e sicurezza online

È il nucleo centrale dell'ePolicy. La normativa impone alle scuole di avere un referente e un protocollo di intervento.

- **Legge 71/2017**: "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo". È la legge quadro che definisce il cyberbullismo e introduce l'ammonimento del Questore.
- **Linee Guida Ministeriali (aggiornamento DM 18/2021)**: forniscono le indicazioni operative per l'aggiornamento dei regolamenti di istituto e la gestione dei casi di bullismo e cyberbullismo.
- **Legge 17 maggio 2024, n. 70**: rafforza le misure di contrasto al bullismo e cyberbullismo, introducendo percorsi rieducativi e una maggiore sorveglianza da parte delle istituzioni scolastiche.

Uso dei dispositivi personali (BYOD) e cellulari

Le regole sull'uso degli smartphone sono diventate molto più stringenti nel biennio 2024–2025.

- **Circolare Ministeriale 11 luglio 2024**: ribadisce il divieto di utilizzo del cellulare durante le lezioni, anche per finalità didattiche, nella scuola primaria e secondaria di primo grado; per le superiori l'uso è consentito esclusivamente sotto la guida del docente per scopi didattici e inclusivi.
- **Nota Ministeriale 19 dicembre 2022**: precorre il divieto attuale, sottolineando come l'uso improprio sia un elemento di distrazione e una mancanza di rispetto.

Valutazione e disciplina (Riforma Valditara 2024/2025)

Le violazioni dell'ePolicy (come riprendere un docente senza consenso o atti di cyberbullismo) incidono pesantemente sul percorso scolastico.

- **Legge 1° ottobre 2024, n. 150 (revisione del voto in condotta)**: con il 5 in condotta scatta la bocciatura automatica; il voto di comportamento influisce sui crediti per l'Esame di Stato; le sospensioni superiori a 2 giorni comportano attività di "cittadinanza solidale" presso strutture convenzionate.

Privacy e protezione dei dati

- **Regolamento UE 2016/679 (GDPR)**: fondamentale per la gestione dei dati personali, delle immagini e dei video realizzati in ambito scolastico.
- **Codice della Privacy (D.Lgs. 196/2003 e successive modifiche)**: regola il trattamento dei dati sensibili degli studenti.

Cittadinanza digitale

- **Legge 92/2019**: introduce l'insegnamento trasversale dell'Educazione Civica, che include espressamente la "Cittadinanza Digitale" come pilastro del curricolo.

Linee guida operative d'Istituto

1. Visione e mission

La nostra scuola riconosce le tecnologie digitali come strumenti fondamentali per l'apprendimento, la ricerca e l'espressione creativa. L'obiettivo è formare cittadini digitali consapevoli, capaci di navigare in rete con spirito critico, etica e responsabilità.

- **Inclusività**: utilizzo delle tecnologie per abbattere barriere e personalizzare l'apprendimento.
- **Responsabilità**: promozione di un ambiente online sicuro, basato sul rispetto reciproco e sulla legalità.
- **Consapevolezza**: sviluppo di competenze per distinguere fonti attendibili da fake news e per proteggere la propria identità digitale.

2. Dotazione tecnologica e rete d'Istituto

L'accesso alle risorse tecnologiche della scuola è un privilegio finalizzato esclusivamente ad attività didattiche e istituzionali.

- **Accesso Wi-Fi**: l'autenticazione alla rete d'istituto avviene tramite credenziali personali. È vietato condividere la propria password o tentare di bypassare i filtri di sicurezza (es. tramite VPN).
- **Monitoraggio**: la scuola si riserva il diritto di monitorare il traffico di rete (nel rispetto della privacy) per scopi di sicurezza e manutenzione.
- **Cura dell'hardware**: gli studenti sono responsabili dell'integrità di PC, tablet e LIM presenti nelle aule e nei laboratori. Eventuali danni tecnici devono essere segnalati immediatamente al docente.

3. Uso dei dispositivi (smartphone e BYOD)

In ottemperanza alla Circolare Ministeriale 11 luglio 2024:

- **Divieto d'uso improprio**: è vietato l'uso del cellulare durante le lezioni, salvo esplicita autorizzazione del docente per scopi didattici o inclusivi.
- **Modalità BYOD (Bring Your Own Device)**: l'uso di dispositivi personali (tablet, PC) è consentito solo se previsto dall'attività didattica programmata e sotto la supervisione del docente.

- **Privacy**: è severamente vietato scattare foto, registrare audio o video all'interno della scuola o durante le attività scolastiche (gite, laboratori) senza il consenso esplicito degli interessati e la finalità didattica approvata.

4. Social media e netiquette

La condotta online riflette la dignità della persona e dell'istituzione scolastica.

- **Identità digitale**: studenti e personale devono evitare di pubblicare contenuti che possano ledere l'immagine dell'Istituto o la reputazione di membri della comunità scolastica.
- **Comunicazione**: nei gruppi di classe (WhatsApp, Telegram, Classroom) è richiesto un linguaggio formale e pertinente. È vietato diffondere materiali coperti da copyright o contenuti inappropriati od offensivi.
- **Diritto all'oblio e disconnessione**: si raccomanda di evitare l'invio di comunicazioni scolastiche fuori dagli orari stabiliti (es. dopo le ore 20:00 o nei giorni festivi), salvo emergenze.

5. Prevenzione e protocollo cyberbullismo

L'Istituto opera attivamente contro ogni forma di prevaricazione online, in linea con la Legge 71/2017 e la Legge 70/2024.

- **Referente di Istituto**: è istituita la figura del Referente per il contrasto al bullismo e cyberbullismo, incaricato di raccogliere segnalazioni.
- **Procedura di segnalazione**: qualsiasi studente, docente o genitore che venga a conoscenza di atti di cyberbullismo (molestie, denigrazione, esclusione, flaming) può segnalarlo tramite il modulo online presente sul sito della scuola o direttamente in vicepresidenza.
- **Supporto**: la scuola attiva percorsi di supporto psicologico e sensibilizzazione tramite il progetto "Safer Internet Centre".

6. Sanzioni e voto in condotta

Il mancato rispetto dell'ePolicy comporta sanzioni disciplinari graduate secondo la gravità dell'infrazione, in linea con la Riforma Valditara (Legge 150/2024).

- **Infrazioni lievi** (es. uso del cellulare senza permesso): sequestro del dispositivo fino al termine delle lezioni e ammonizione scritta.

- **Infrazioni gravi** (es. cyberbullismo, violazione della privacy, diffusione di materiale offensivo): incidenza diretta sul voto in condotta (possibilità di assegnazione del 5 con conseguente non ammissione alla classe successiva o all'Esame di Stato); sospensione dalle lezioni con obbligo di svolgimento di attività di "cittadinanza solidale" presso enti convenzionati; segnalazione alle autorità competenti (Polizia Postale) nei casi previsti dalla legge.

Netiquette di classe: 10 regole d'oro

> *Il rispetto non ha filtri, la tua impronta digitale è per sempre.*

1. **Chiedi prima di scattare**: non fotografare o registrare compagni o docenti senza il loro consenso esplicito e quello del professore per fini didattici. La privacy è un diritto, non un'opzione.
2. **Il cellulare non è un compagno di banco**: durante la lezione il telefono resta nello zaino o nell'apposito contenitore. Usalo solo se il docente lo richiede per un'attività specifica.
3. **Pensa prima di postare**: una foto o un commento inviati "per scherzo" in un gruppo privato possono diventare pubblici in un secondo. Rifletti sulle conseguenze a lungo termine.
4. **No al linguaggio d'odio (hate speech)**: non insultare, non denigrare e non escludere nessuno dai gruppi di classe. Il bullismo online ha lo stesso peso (e sanzioni) di quello fisico.
5. **Rispetta l'orario di disconnessione**: evita di inviare messaggi relativi alla scuola o ai compiti dopo le ore 20:00 o nei weekend, a meno che non sia urgente. Tutti hanno diritto al riposo.
6. **Verifica le fonti**: prima di condividere una notizia o un file "clamoroso", controlla che sia vero. Non diventare un moltiplicatore di fake news.
7. **Proteggi le tue credenziali**: la tua password d'istituto è personale. Non cederla a nessuno e non usare account altrui per inviare messaggi o compiti.
8. **Usa un tono appropriato**: nei gruppi di classe e nelle email ai docenti usa un linguaggio educato e corretto. Scrivere a un "prof" non è come scrivere a un amico in chat.
9. **Segnala, non guardare e basta**: se vedi un compagno in difficoltà o vittima di attacchi online, parlane con un docente o con il Referente Cyberbullismo. Il silenzio è complicità.
10. **Sii un cittadino, non solo un utente**: usa la rete per costruire, imparare e condividere valore, non per distruggere la reputazione altrui.

Capitolo 1 – Introduzione al documento di ePolicy

Scopo dell'ePolicy

Le TIC (Tecnologie dell'Informazione e della Comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse. Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006, aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

In un contesto sempre più complesso diventa essenziale per ogni Istituto scolastico dotarsi di una ePolicy, un documento programmatico volto a promuovere le competenze digitali e un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze sia degli adulti coinvolti nel processo educativo. L'ePolicy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati a un utilizzo scorretto degli strumenti.

L'ePolicy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa in riferimento alle tecnologie digitali. Nello specifico:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione rispetto ai comportamenti online a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate a un uso non corretto delle tecnologie digitali.

Perché è importante dotarsi di una ePolicy?

Attraverso l'ePolicy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.

L'ePolicy fornisce, quindi, delle linee guida per garantire il benessere in rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative ed educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

Ruoli e responsabilità

Affinché l'ePolicy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, s'impegni nell'attuazione e promozione di essa.

Il Dirigente Scolastico è garante della sicurezza, anche online, di tutti i membri della comunità scolastica. Può promuovere la cultura della sicurezza online e, ove possibile, dare il proprio contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC. Ha anche la responsabilità di gestire e intervenire nei casi di gravi episodi di bullismo, cyberbullismo e uso improprio delle tecnologie digitali.

L'Animatore digitale supporta il personale scolastico dal punto di vista tecnico-informatico e in riferimento ai rischi online, alla protezione e gestione dei dati personali, oltre a essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica); monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola e ha il compito di controllare che gli utenti autorizzati accedano alla rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

Il Referente cyberbullismo ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Fondamentale, dunque, il suo ruolo non solo in ambito scolastico ma anche in quello extrascolastico, in quanto (ove possibile) potrebbe coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.

I Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della rete. Possono integrare parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica. I docenti accompagnano e supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici connessi alla rete; hanno il

dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che veda coinvolti studenti e studentesse.

Il personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste, di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il Dirigente Scolastico e con tutto il personale docente. Diverse figure che, in sinergia, si occupano, ciascuna per la propria funzione, del funzionamento dell'Istituto scolastico, che passa anche attraverso lo sviluppo della cultura digitale e l'organizzazione del tempo scuola. Esiste un concreto coinvolgimento del personale ATA nell'applicazione della Legge 107/15 ("La Buona Scuola"), che concerne non solo il tempo scuola e il potenziamento dell'offerta formativa, ma anche le attività di formazione e autoformazione in tema di bullismo e cyberbullismo. Il personale ATA dovrebbe, all'interno dei singoli regolamenti d'Istituto, essere coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure, e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

Gli Studenti e le Studentesse sono invitati, in relazione al proprio grado di maturità e consapevolezza raggiunta, a utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola devono imparare a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/e; partecipano attivamente a progetti e attività che riguardano l'uso positivo delle TIC e della rete e si fanno promotori di quanto appreso anche attraverso possibili percorsi di peer education.

I Genitori, in continuità con l'Istituto scolastico, sono invitati a essere partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della rete, nonché sull'uso responsabile dei device personali; sono tenuti a relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la rete e a comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet. È estremamente importante che leggano e condividano quanto scritto nell'ePolicy dell'Istituto.

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola si devono conformare alla politica della stessa riguardo all'uso consapevole della rete e delle TIC; devono inoltre promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

Informativa per i soggetti esterni che erogano attività educative nell'Istituto

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati; essere guidati dal principio dell'interesse superiore del minore; ascoltare e prendere in seria considerazione le opinioni e i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse, oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali o abusivi o che mettano a rischio la loro sicurezza.

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto, dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, PC, ecc.) e di quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, email, chat, profili di social network).

Qualora si verificassero problematiche relative all'uso non corretto delle tecnologie digitali o si avesse un sospetto di forme di maltrattamento/abuso, sia nel reale sia nel virtuale, sia dal punto di vista fisico sia psicologico, a danno di minori, si chiede ai soggetti esterni che erogano attività educative nell'Istituto di rifarsi alle procedure allegate all'ePolicy e al Regolamento d'Istituto.

Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

Il documento di ePolicy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/alle studenti/esse) si faccia a sua volta promotore del documento.

L'ePolicy viene condivisa e comunicata al personale, agli studenti e alle studentesse e alla comunità scolastica attraverso la pubblicazione del documento sul sito istituzionale della scuola e il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico.

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di PC collegati alla rete o comunque in vari punti dell'Istituto. Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e

supportati nella navigazione online negli spazi della scuola e sulle regole di condotta da tenere in rete.

Gestione delle infrazioni alla ePolicy

La scuola gestirà le infrazioni all'ePolicy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

Integrazione dell'ePolicy con i regolamenti esistenti

Il Regolamento dell'Istituto scolastico viene aggiornato con specifici riferimenti all'ePolicy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida MIM e le indicazioni normative generali sui temi in oggetto. Una volta approvata l'ePolicy, verranno aggiornati il Regolamento d'Istituto e il Patto di Corresponsabilità.

Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'ePolicy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

Il nostro piano d'azioni (1)

Azioni da sviluppare nell'anno scolastico 2025/2026

- Creazione del gruppo di lavoro ePolicy.
- Attivazione dell'account email **epolicy@istitutostradivari.it** (e/o segnalazioni@ o bullismo@) per informazioni e segnalazioni.
- Integrazione dell'ePolicy nei documenti dell'Istituto.
- Presentazione e approvazione dell'ePolicy ai docenti dell'Istituto durante il Collegio Docenti di maggio 2026.
- Diffusione dell'ePolicy nel contesto scolastico, a studenti e studentesse, docenti, personale ATA e famiglie, attraverso materiale informativo user friendly (video, slide, flashcard) su sito web della scuola e canali di comunicazione scolastici.

Azioni da sviluppare nel triennio successivo

- Aggiornamento periodico del documento e del materiale informativo sulla base delle novità digitali e dei monitoraggi interni.
- Presentazione annuale dell'aggiornamento dell'ePolicy ai docenti dell'Istituto durante il Collegio Docenti (data da definire o evento annuale dedicato).
- Creazione di materiali semplificati (poster, infografiche) per gli studenti da parte degli studenti stessi (peer education).

Capitolo 2 – Formazione e curricolo

Curricolo sulle competenze digitali per gli studenti e DigComp 3.0

I ragazzi usano la rete quotidianamente, talvolta in modo più "intuitivo" e "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali".

Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico" (Raccomandazione del Consiglio europeo relativa alle competenze chiave per l'apprendimento permanente, C189/9, p. 9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse a un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale. Saranno presi in considerazione i documenti più importanti per progettare e implementare un buon curricolo sulle competenze digitali, tra cui:

- Piano Nazionale Scuola Digitale (PNSD), in particolar modo il paragrafo 4.2 su "Competenze e contenuti";
- Sillabo sull'Educazione Civica Digitale;
- DigComp 3.0;
- Raccomandazione del Consiglio europeo relativa alle competenze chiave per l'apprendimento permanente (C189/9, p. 9).

Le versioni del DigComp: dalla 1.0 alla 3.0

DigComp 1.0 del 2013 e 2.0 del 2016 hanno gettato le fondamenta, identificando le cinque aree di competenza e le ventuno competenze specifiche che costituiscono ancora oggi l'ossatura del framework. Nel 2017, DigComp 2.1 ha introdotto la granularità degli otto livelli di padronanza, rendendo il quadro uno strumento preciso per la valutazione. La versione 2.2 del 2022 ha aperto le

porte all'intelligenza artificiale, introducendo i primi riferimenti espliciti, seppur in modo ancora limitato.

Il DigComp 3.0, presentato a fine 2025, è l'ultima evoluzione del quadro europeo per le competenze digitali. Aggiorna il precedente DigComp 2.2 per rispondere alle sfide tecnologiche attuali, integrando trasversalmente l'intelligenza artificiale (IA), la cybersicurezza avanzata, il benessere digitale, la sostenibilità e i diritti dei cittadini nell'era dell'IA. DigComp 3.0 definisce le competenze digitali essenziali per vivere, lavorare e partecipare alla società europea contemporanea. Come nelle versioni precedenti, il modello si basa su cinque aree di competenza.

Area 1 – Alfabetizzazione su informazioni e dati

Questa prima area si concentra sulla capacità di articolare bisogni informativi e di cercare, localizzare e recuperare informazioni e contenuti digitali. L'aggiornamento introduce una forte enfasi sulla gestione critica delle informazioni, competenza divenuta essenziale nell'era della sovrabbondanza informativa e della disinformazione. Gli studenti devono imparare non solo a trovare informazioni, ma anche a valutare criticamente le fonti, interpretare i contenuti digitali e comprendere i processi utilizzati per generarli, inclusi quelli basati sull'intelligenza artificiale. Questa area include anche la capacità di organizzare, archiviare, gestire e analizzare dati e informazioni in ambienti digitali strutturati.

Area 2 – Comunicazione e collaborazione

La seconda area si estende ben oltre la semplice capacità di inviare messaggi digitali. Comprende l'interazione attraverso diverse tecnologie digitali, la condivisione etica e responsabile di informazioni, la partecipazione alla cittadinanza attraverso piattaforme e servizi digitali e la collaborazione per la co-costruzione di conoscenze e risorse. Una novità significativa riguarda la gestione dell'identità digitale in contesti sempre più complessi, dove gli studenti devono imparare a curare la propria presenza online, proteggere la propria reputazione digitale e comprendere le implicazioni della propria impronta digitale. L'area include anche la consapevolezza delle norme comportamentali appropriate negli ambienti digitali e il rispetto della diversità culturale, generazionale e di altro tipo.

Area 3 – Creazione di contenuti digitali

Quest'area integra pienamente l'uso di strumenti di intelligenza artificiale generativa per la creazione e modifica di contenuti digitali. Gli studenti devono comprendere come modificare, perfezionare e integrare nuove informazioni in corpi di conoscenza esistenti per creare contenuti

originali. Fondamentale è anche la comprensione di come si applicano diritti d'autore e licenze, con particolare attenzione alle questioni legali ed etiche emergenti legate all'uso dell'intelligenza artificiale nella creazione di contenuti. L'area include inoltre il pensiero computazionale e la programmazione, competenze che permettono di comprendere e implementare i passaggi necessari per analizzare un problema e sviluppare una sequenza di istruzioni per un sistema informatico.

Area 4 – Sicurezza, benessere e uso responsabile

Questo è uno dei cambiamenti più significativi rispetto alle versioni precedenti. Il titolo stesso dell'area (prima era semplicemente "Sicurezza") riflette un'evoluzione importante: ora include esplicitamente il benessere psicofisico degli individui e l'impatto ambientale delle tecnologie digitali. Gli studenti devono imparare a proteggere dispositivi, contenuti e dati personali, ma anche a sostenere il proprio benessere fisico, mentale e sociale nell'uso delle tecnologie. L'area comprende la consapevolezza dei benefici e dei rischi delle tecnologie digitali per il benessere e l'inclusione sociale, inclusa la capacità di bilanciare l'uso delle tecnologie digitali con attività offline. Una novità assoluta è l'attenzione all'impatto ecologico del digitale: gli studenti devono comprendere che ogni click, ogni video in streaming e ogni modello di intelligenza artificiale addestrato ha un costo energetico misurabile.

Area 5 – Identificazione e risoluzione di problemi

La quinta area aggiunge "Identificazione" al titolo precedente, sottolineando che saper riconoscere un problema (anche etico o sociale) è importante quanto saperlo risolvere. Quest'area comprende la capacità di identificare e valutare bisogni e di utilizzare le tecnologie digitali per soddisfarli, adattando gli ambienti digitali ai contesti, agli obiettivi e alle esigenze proprie e altrui. Include anche la risoluzione di problemi tecnici e concettualmente complessi, l'uso creativo delle tecnologie digitali per migliorare processi e prodotti esistenti o creare nuove soluzioni, e la capacità di costruire autonomia operativa negli ambienti digitali. Fondamentale è anche rimanere informati sugli sviluppi tecnologici digitali e sulle loro implicazioni personali, professionali e sociali.

La versione 3.0 aggiorna descrittori, esempi e livelli di padronanza, integrando diversi aspetti come:

- uso responsabile e consapevole dell'IA generativa;
- verifica e affidabilità delle informazioni digitali;
- sicurezza avanzata, privacy e gestione dell'identità digitale;

- competenze per l'interoperabilità dei dati e la sostenibilità ambientale del digitale;
- capacità di risolvere problemi in contesti tecnologici complessi.

Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica

È fondamentale che tutti i docenti siano formati e aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo e inclusivo. Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti. L'Istituto si prefigge di riconoscere e favorire la partecipazione del personale a iniziative promosse sia direttamente dalla scuola, dalle reti di scuole e dall'amministrazione, sia a quelle liberamente scelte dai docenti (anche online), coerenti con il piano di formazione. L'Istituto consente in questo modo di sviluppare capacità sempre più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza e il confronto fra pari in modalità asincrona.

Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza periodica, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e, se necessario, di personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole polo, ecc.), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Nella prevenzione dei rischi connessi a un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie su tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso

l'aggiornamento, oltre che del Regolamento scolastico, anche del Patto di Corresponsabilità e attraverso una sezione dedicata sul sito web dell'Istituto.

Il nostro piano d'azioni (2)

Azioni da sviluppare nell'anno scolastico 2025/2026

- **Analizzare il fabbisogno formativo dei docenti** (test, autovalutazione, raccolta interessi) sull'utilizzo delle TIC nella didattica e sull'uso consapevole della rete.
- Aggiornare il curricolo digitale e la relativa griglia di valutazione sulla base del **DigComp 3.0**.

Azioni da sviluppare nel triennio successivo

- **Analizzare il fabbisogno degli studenti** sulle competenze digitali.
- Strutturare e implementare il curricolo verticale di educazione civica integrando nuove offerte formative sull'educazione digitale.
- Organizzare attività di formazione sulle applicazioni disponibili nel nostro Istituto (**Canva, Google Workspace**, con un focus specifico su **Notebook LM**) per gli studenti delle classi prime durante la settimana dell'accoglienza, al fine di favorire un uso consapevole ed efficace degli strumenti digitali.
- Organizzare per i docenti corsi su TIC e didattica innovativa, formazione base e avanzata su IA, sicurezza e cittadinanza digitale, in base alle priorità emerse dall'analisi del fabbisogno, anche attraverso la partecipazione a progetti specifici come il PNRR AI.
- Integrare le competenze digitali nella didattica disciplinare.
- Predisporre un **kit didattico**, costituito da una raccolta di moduli operativi e buone pratiche, da mettere a disposizione dei docenti per la realizzazione di attività educative significative durante le ore di alternativa/supplenza.
- Monitorare e valutare periodicamente le competenze digitali degli studenti.

Capitolo 3 – Gestione dell'infrastruttura e della strumentazione ICT

Protezione dei dati personali

> *"Le scuole sono chiamate ogni giorno ad affrontare la sfida più difficile, quella di educare le nuove generazioni non solo alla conoscenza di nozioni basilari e alla trasmissione del sapere, ma soprattutto al rispetto dei valori fondanti di una società. Nell'era di Internet e in presenza di nuove forme di comunicazione questo compito diventa ancora più cruciale. È importante riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino."*
>
> *(Garante per la protezione dei dati personali – garanteprivacy.it/temi/scuola)*

Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali. Il corretto trattamento dei dati personali a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni.

La protezione dei dati personali è un diritto fondamentale di ogni individuo, tutelato a livello europeo dal Regolamento (UE) 2016/679 (GDPR) e, in Italia, dal D.Lgs. 101/2018. In ambito scolastico essa rappresenta una condizione necessaria per rispettare la dignità, l'identità e il diritto alla riservatezza di studenti, famiglie e personale.

Che cosa sono i dati personali?

Sono tutte quelle informazioni che identificano o rendono identificabile una persona fisica. Si distinguono diverse categorie:

- **Identificazione diretta**: dati anagrafici come nome e cognome.
- **Identificazione indiretta**: codici identificativi come il codice fiscale, l'indirizzo IP o il numero di targa.

- **Categorie particolari (dati sensibili)**: informazioni che rivelano l'origine razziale o etnica, convinzioni religiose, opinioni politiche, dati relativi alla salute, alla vita o all'orientamento sessuale, nonché dati genetici e biometrici.
- **Dati giudiziari**: relativi a condanne penali e reati.
- **Dati digitali**: informazioni derivanti dalle comunicazioni elettroniche e dalla geolocalizzazione.

Il "trattamento" dei dati

Per trattamento si intende qualsiasi operazione applicata ai dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'uso, la comunicazione o la cancellazione. Chi tratta i dati deve adottare misure tecniche e organizzative idonee a garantirne la sicurezza.

Le figure coinvolte

- **Interessato**: la persona fisica a cui si riferiscono i dati.
- **Titolare**: l'ente o la persona (ad esempio la scuola) che decide le finalità e le modalità del trattamento.
- **Responsabile**: il soggetto che esegue il trattamento per conto del titolare.

Gli obblighi della scuola

Le istituzioni scolastiche gestiscono quotidianamente numerosi dati, spesso sensibili (come problemi sanitari o disagi sociali). Per essere in regola con la normativa, la scuola deve:

- trattare solo i dati necessari per **finalità istituzionali**;
- redigere e mantenere un **registro dei trattamenti**;
- fornire agli interessati un'adeguata **informativa** e, dove previsto, richiedere il consenso;
- garantire i diritti degli interessati, tra cui l'accesso, la rettifica, la cancellazione (diritto all'oblio) e l'opposizione al trattamento.

Per tale ragione tutte le scuole, e quindi anche l'Istituto Stradivari, hanno una sezione del proprio sito istituzionale (Privacy) che raccoglie tutte le informazioni su come si opera per una corretta protezione, conservazione e trattamento dei dati personali di tutte le componenti della scuola (docenti, studenti, famiglie, personale interno, collaboratori esterni, fornitori, ecc.), nel rispetto del Regolamento dell'Unione Europea 2016/679 (GDPR): Sezione Privacy dell'Istituto Stradivari

Particolare attenzione è rivolta ai minori: la scuola ha il compito non solo di tutelarne la privacy, ma anche di educarli a proteggere la propria riservatezza online, specialmente nell'uso di smartphone, social network e strumenti didattici digitali.

Informative sul trattamento dei dati personali (art. 13 Regolamento UE 2016/679)

Le informative vengono fornite:

- al momento dell'iscrizione degli allievi, ai rispettivi genitori (o a chi ne esercita la potestà);
- sul diario scolastico, annualmente consegnato ad allievi e genitori; particolare attenzione viene prestata alla normativa sulla diffusione di immagini, video e materiale multimediale e sulla trasmissione di documenti e certificazioni sanitarie;
- al momento della sottoscrizione del contratto di lavoro e/o d'incarico (cfr. Registro delle attività di trattamento); vengono fornite, su supporto cartaceo, istruzioni particolareggiate nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione, e ciclicamente la scuola organizza corsi di aggiornamento a riguardo;
- a tutto il personale scolastico; in particolare, agli autorizzati al trattamento: soggetti interni (dipendenti e assimilati) che trattano dati in nome e per conto del titolare;
- ai responsabili del trattamento: soggetti esterni che trattano dati in nome e per conto del titolare, con loro organizzazione autonoma in forza di un contratto.

Accesso a Internet e sicurezza online

> *"L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale. Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale. Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla rete. L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite. Le istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale, tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità."*

L'accesso ad Internet non è considerato solo un servizio tecnico, ma un vero e proprio diritto fondamentale della persona, indispensabile per il pieno sviluppo individuale e sociale di ogni cittadino, e la scuola gioca un ruolo cruciale nel garantire che questo diritto diventi effettivo per tutti gli studenti.

Un diritto per superare il divario digitale

Il diritto di accesso deve essere assicurato in condizioni di parità, rimuovendo gli ostacoli economici e sociali. Le istituzioni pubbliche, tra cui la scuola, hanno il compito di intervenire per superare ogni forma di divario digitale (digital divide), sia esso legato al genere, alle condizioni economiche o a situazioni di vulnerabilità e disabilità. La scuola deve essere il luogo dove questo accesso è garantito anche a chi non dispone di una connessione a casa.

Sicurezza online: safety vs security

La scuola deve garantire un ambiente sicuro, distinguendo tra due tipi di protezione:

- **Safety**: riguarda la prevenzione dei rischi e la preparazione degli utenti verso un uso consapevole delle tecnologie.
- **Security**: riguarda le risorse tecnologiche hardware e software (antivirus, firewall, protocolli https, gestione degli account) che rendono tecnicamente sicuro l'ambiente digitale.

Infrastruttura e obiettivi del PNSD

L'Istituto Stradivari dispone di un server fisico, con diversi Windows Server 2016 virtuali con compiti di gestione della didattica, degli uffici di segreteria e dei servizi. Questi gestiscono in modo centralizzato utenti, computer e permessi, garantendo che ogni risorsa sia sicura e accessibile solo a chi ne ha diritto. Oltre ad Active Directory, il server ospita servizi di rete critici che assicurano la connettività e la conformità degli standard su tutti i dispositivi connessi. Un sistema di backup giornaliero è attivo su una stazione NAS e su cloud. I computer degli uffici sono protetti da antivirus Managed Endpoint Detection and Response (MDR) Malwarebytes con licenza a pagamento. La protezione e sicurezza in rete è affidata a un firewall che ha il compito di:

- analizzare ogni dato che prova a entrare nella rete scolastica: se riconosce un virus, un malware o un tentativo di intrusione, gli sbarra la strada immediatamente, impedendo che i computer della scuola vengano danneggiati;

- assicurarsi che gli studenti non finiscano su siti pericolosi o non adatti alla loro età: se qualcuno prova a digitare l'indirizzo di un sito vietato, il firewall visualizza una pagina di blocco, proteggendo la navigazione dei ragazzi;
- creare dei "muri invisibili" tra la rete usata dalla segreteria (dove ci sono i voti e i dati sensibili) e quella del laboratorio di informatica o del Wi-Fi per gli ospiti, evitando che occhi indiscreti accedano a informazioni private;
- evitare che la connessione rallenti troppo: ad esempio, può limitare la banda per i video in streaming durante le ore di lezione, dando la precedenza alle piattaforme didattiche.

In linea con il Piano Nazionale Scuola Digitale (PNSD), il nostro Istituto è dotato di una connessione in fibra ottica a banda ultralarga. Questo permette l'accesso diffuso (tramite cablaggio LAN e wireless) in ogni aula, laboratorio e spazio comune. Sono state configurate reti Wi-Fi diverse per consentire l'accesso alle diverse tipologie di utenti:

- "Liuteria", "Artistico", "WIFI-Moda" per la didattica di docenti e studenti;
- "Liuteria-Ospiti", "Artistico-Ospiti", "Moda-Ospiti" per gli operatori e i collaboratori esterni;
- gli uffici amministrativi, presenti solo nella sede centrale, utilizzano una rete cablata, separata dalle altre, per una maggiore sicurezza.

L'autorizzazione all'accesso alla rete Wi-Fi dell'Istituto viene concessa a tutto il personale in servizio, agli studenti e a quanti ne fanno richiesta per esigenze legate allo svolgimento di particolari attività/progetti. L'accesso viene consentito anche a personale esterno che svolge specifiche attività all'interno dell'Istituto (es. esperti esterni, educatori, ecc.).

L'Istituto è registrato alla piattaforma Google Workspace: questo permette l'utilizzo di tutta la suite di Google per l'elaborazione di testi, immagini e fogli di lavoro, la gestione di spazio su cloud e Classroom per il lavoro collaborativo nelle classi. Lo scambio di informazioni tra scuola e famiglia avviene attraverso strumenti come il registro elettronico Mastercom e la normale posta elettronica. La Segreteria utilizza il software della ditta Spaggiari per la gestione totalmente digitale di tutta la documentazione scolastica: fascicoli personali di studenti e personale, archivi contabili, ecc.

Regolamentazione e PUA (Politica di Uso Accettabile)

L'accesso alla rete a scuola non è libero da regole. L'Istituto si dota di strumenti specifici.

Regolamento d'Istituto sulle TIC: elenca puntualmente le "regole di ingaggio" per docenti, personale e studenti. Tra queste spicca in particolare quella avente ad oggetto: "Linee di indirizzo

ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, dovere di vigilanza e di corresponsabilità dei genitori e dei docenti".

PUA (Politica di Uso Accettabile): definisce cosa è consentito e cosa è vietato durante la navigazione. La PUA regolamenta l'uso dell'indirizzo di posta elettronica personale fornito dalla scuola a studenti e docenti. Questi account, collegati a Google Workspace, devono essere utilizzati esclusivamente per accedere alle piattaforme e-learning e per le attività didattiche; è esplicitamente vietato usarli per registrarsi su social network o piattaforme di gioco personali. Il documento definisce la durata degli accessi, stabilendo che l'account rimanga attivo solo per il tempo di permanenza nell'Istituto (con una scadenza tipica al 31 agosto dell'anno di fine percorso). La stesura della PUA è prevista come azione necessaria per integrare il Patto di Corresponsabilità tra scuola e famiglia, assicurando che tutti gli attori siano consapevoli delle proprie responsabilità online.

Netiquette: un insieme di regole di comportamento (galateo della rete), spesso elaborate con la collaborazione degli studenti, per una convivenza civile online. Nelle chat di gruppo (come WhatsApp o Telegram) tra colleghi o tra docenti e genitori si suggerisce quanto segue:

- **Pertinenza**: scrivere e pubblicare solo contenuti coerenti con le finalità del gruppo.
- **Linguaggio chiaro**: usare termini precisi, poiché la comunicazione online è priva di segnali non verbali (tono, espressioni) e si presta a facili malintesi.
- **Gestione dei contenuti**: evitare di affrontare in chat argomenti troppo complessi o controversi, che è meglio discutere di persona o nei consigli di classe.
- **Rispetto degli altri**: evitare discussioni private che coinvolgono solo pochi interlocutori all'interno di un gruppo numeroso.
- **Sintesi**: indirizzare domande chiare e brevi, evitando messaggi troppo spezzettati.
- **Privacy e sicurezza**: non condividere file troppo pesanti e, soprattutto, non condividere foto di studenti nelle chat informali.
- **Diritto alla disconnessione**: aspetto fondamentale della netiquette scolastica, serve a conciliare la vita lavorativa con quella familiare, evitando l'invio di messaggi o l'uso di strumentazioni tecnologiche al di fuori dell'orario di servizio.

Impegni e responsabilità

- **Gli studenti** si impegnano a utilizzare la rete correttamente, rispettare le consegne dei docenti, non scaricare materiale non autorizzato e segnalare immediatamente contenuti inadeguati.
- **I docenti** hanno il compito di monitorare l'uso che gli studenti fanno delle tecnologie e di formarli a una navigazione sicura e critica, distinguendo ad esempio tra notizie vere e fake news.
- **La scuola** adotta sistemi di filtraggio (firewall hardware) per evitare l'accesso a materiali non adatti all'età dei minori.

In sintesi, l'accesso a Internet a scuola è finalizzato a sviluppare una cultura digitale diffusa, rendendo l'ambiente di apprendimento aperto, flessibile e inclusivo, preparando al contempo i ragazzi alle sfide del futuro mercato del lavoro.

Strumenti di comunicazione online

Gli strumenti di comunicazione online a scuola hanno l'obiettivo di ridefinire gli ambienti di apprendimento, rendendo lo scambio di informazioni più interattivo, orizzontale e collaborativo. Si distingue innanzitutto tra comunicazione interna ed esterna.

- **Comunicazione interna ed esterna**: per raggiungere soggetti esterni (famiglie, istituzioni) o far circolare informazioni di servizio tra docenti, studenti e genitori.
- **Registro elettronico**: è lo strumento centrale per la gestione di assenze, voti, comunicazioni di classe, prenotazione di colloqui e condivisione di documenti di valutazione.
- **Piattaforme di lavoro collaborativo**: strumenti come Google Workspace for Education (che include Classroom, Google Documenti e posta elettronica personale) e altri applicativi cloud che facilitano la didattica partecipata.
- **Messaggistica istantanea**: gruppi su applicazioni come WhatsApp, utilizzati prevalentemente per comunicazioni rapide e informali tra colleghi o tra docenti e genitori.

Dispositivi personali (BYOD)

La strumentazione personale all'interno della scuola si inserisce principalmente nel quadro del BYOD (Bring Your Own Device), una metodologia che prevede l'uso di dispositivi digitali di proprietà degli studenti per fini didattici.

Tipologie di dispositivi

- **Smartphone**: come stabilito dal Ministero dell'Istruzione con la Direttiva n. 30/2007 e dalla Circolare Ministeriale 3392/2025, è vietato utilizzare lo smartphone durante tutto l'orario scolastico (pause, spostamenti e ricreazione compresi). L'uso del telefono cellulare è ammesso nei casi in cui sia previsto dal Piano Educativo Individualizzato o dal Piano Didattico Personalizzato come supporto agli alunni con bisogni educativi speciali, ovvero per motivate e certificate necessità personali.
- **Tablet**: impiegati per la consultazione di libri elettronici e testi online, per prendere appunti e, nel caso degli studenti di grafica e moda, per realizzare disegni artistici a mano libera, figurini di stile e modelli di abbigliamento.
- **Computer personali (PC)**: utilizzabili in gruppo o singolarmente per attività di collaborazione, studio e ricerca.

Regole per l'utilizzo a scuola

- **Finalità esclusivamente didattiche**: i dispositivi possono essere accesi e utilizzati solo quando richiesto dal docente per specifiche attività di apprendimento.
- **Dispositivi spenti**: al di fuori delle attività didattiche autorizzate, lo smartphone deve essere tenuto spento.
- **Consenso del docente**: l'uso di cellulari e smartphone per fini personali, come ad esempio registrare una lezione, è consentito solo previo consenso esplicito del docente e nel rispetto della privacy altrui.
- **Divieto di diffusione**: è severamente vietato acquisire o divulgare immagini, filmati o registrazioni vocali senza autorizzazione; la violazione di tale norma può comportare sanzioni civili, penali e disciplinari.

Strumenti forniti dall'Istituto

- **Account istituzionale**: ogni studente riceve un indirizzo di posta elettronica personale (collegato a Google Workspace for Education).
- **Accesso al cloud**: l'account permette l'accesso a piattaforme e-learning e strumenti di archiviazione cloud per svolgere le attività scolastiche.

Responsabilità

- **Studenti**: devono rispettare le "regole di ingaggio", evitando usi impropri come chattare, giocare o navigare sui social durante le lezioni.

- **Genitori**: hanno il compito di vigilare sull'uso degli account scolastici a casa, assicurandosi che vengano utilizzati solo per scopi didattici.
- **Docenti**: monitorano l'uso delle tecnologie in classe e formano gli studenti a un utilizzo critico e responsabile.

Altri aspetti sull'utilizzo dei dispositivi personali da parte degli alunni sono disciplinati anche in considerazione dei 10 punti del MIUR per l'uso dei dispositivi mobili a scuola: Decalogo BYOD del MIM.

Il nostro piano d'azioni (3)

Azioni da sviluppare nell'anno scolastico 2025/2026 (almeno una tra le seguenti)

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte di studenti e studentesse, dei docenti o del personale tecnico-amministrativo e ATA;
- organizzare eventi o attività di consultazione di docenti, studenti/studentesse o genitori per redigere o integrare indicazioni e regolamenti sull'uso dei dispositivi digitali personali a scuola;
- organizzare eventi o attività di formazione, rivolti al personale adulto, agli studenti e alle studentesse o ai genitori, sul tema delle tecnologie digitali e della protezione dei dati personali;
- organizzare eventi o attività di formazione, rivolti al personale adulto, agli studenti e alle studentesse, sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity).

Azioni da sviluppare nel triennio successivo (almeno una per anno)

- Proseguire e consolidare le medesime tipologie di azioni (analisi sull'utilizzo dei dispositivi, consultazioni della comunità scolastica, formazione su protezione dei dati personali e cybersecurity), selezionando almeno un'azione per ciascun anno scolastico in base alle priorità emerse.

Capitolo 4 – Rischi online: conoscere, prevenire e rilevare

Sensibilizzazione e prevenzione

Il rischio online si configura come la possibilità per il minore di: commettere azioni online che possano danneggiare sé stessi o altri; essere una vittima di queste azioni; osservare altri commettere queste azioni.

È importante riconoscere questi fenomeni e saperli distinguere tra loro in modo da poter adottare le strategie migliori per arginarli e contenerli, ma è altrettanto importante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano. Ciò è possibile lavorando su aspetti di ampio raggio che possano permettere una riduzione dei fattori di rischio e, di conseguenza, una minore probabilità che i ragazzi si trovino in situazioni non piacevoli. È importante che abbiano gli strumenti idonei per riconoscere possibili situazioni di rischio e segnalarle a un adulto di riferimento.

Gli strumenti da adottare per ridurre l'incidenza di situazioni di rischio si configurano come interventi di sensibilizzazione e prevenzione.

- **Sensibilizzazione**: azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.
- **Prevenzione**: insieme di attività, azioni e interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale, riducendo quindi i rischi per la sicurezza di bambine/i e ragazze/i.

La Commissione Cyberbullismo, in tal senso, si occupa di sensibilizzare e prevenire il fenomeno del cyberbullismo con interventi nelle classi a carattere preventivo, con particolare riferimento alla differenza tra bullismo e cyberbullismo, alla diversità, all'importanza dell'empatia e alla forza del gruppo.

Cyberbullismo: che cos'è e come prevenirlo

La Legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", all'art. 1, comma 2, definisce il cyberbullismo:

> *"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti online aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo".*

Nell'ambito delle istituzioni scolastiche, la Legge 70/2024 prevede, in aggiunta a quanto stabilito dalla Legge 71/2017 e dalle Linee di Orientamento per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo emanate dal Ministero dell'Istruzione e del Merito nel 2021, ulteriori obblighi. Le azioni poste a carico dei Dirigenti Scolastici risultano essere, a oggi, le seguenti:

- definire le linee di indirizzo del Piano Triennale dell'Offerta Formativa (PTOF) e del Patto di Corresponsabilità Educativa affinché contemplino misure dedicate alla prevenzione dei fenomeni di bullismo e cyberbullismo;
- nominare un referente per il bullismo e cyberbullismo;
- curare l'adozione di un codice interno per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo;
- istituire un tavolo permanente di monitoraggio del quale fanno parte rappresentanti degli studenti, degli insegnanti, delle famiglie ed esperti di settore;
- elaborare, in collaborazione con il/i referente/i per il bullismo e il cyberbullismo, un Regolamento condiviso per il contrasto dei fenomeni di bullismo e cyberbullismo, che preveda sanzioni in un'ottica di giustizia riparativa e forme di supporto alle vittime; il Regolamento deve essere esplicitato nel Patto di Corresponsabilità Educativa firmato dai genitori e i suoi contenuti vanno condivisi e approvati dal Consiglio d'Istituto;
- promuovere interventi di prevenzione primaria e, per le scuole secondarie, sollecitare il coinvolgimento attivo degli studenti anche attraverso modalità di peer education;
- promuovere attività di formazione/informazione rivolte a docenti, studenti, famiglie e personale ATA;
- organizzare e coordinare i Team Antibullismo e per l'Emergenza;
- predisporre eventuali piani di sorveglianza in funzione delle necessità della scuola;
- fornire, tramite il sito web della scuola, informazioni su: nominativo/i del/i referente/i per il bullismo e cyberbullismo; contenuti informativi su azioni e attività di contrasto ai fenomeni

di bullismo e cyberbullismo (Regolamento d'Istituto, PTOF, Patto di Corresponsabilità) oltre che di educazione digitale;

- attivare un sistema di segnalazione nella scuola;
- attivare uno sportello psicologico e un centro di ascolto gestito da personale specializzato (psicologi presenti nell'istituto o nei servizi del territorio), anche in collaborazione con i servizi pubblici territoriali; ove non sia possibile attuare tali condizioni, anche tramite reti di scuole;
- qualora venga a conoscenza di atti di bullismo o cyberbullismo che coinvolgano studenti iscritti all'istituto, salvo che il fatto costituisca reato, informare tempestivamente i genitori dei minori coinvolti o i soggetti esercenti la responsabilità genitoriale e promuovere adeguate iniziative di carattere educativo nei riguardi dei minori medesimi, anche con l'eventuale coinvolgimento del gruppo classe in percorsi di mediazione scolastica;
- nei casi più gravi, ovvero se si tratti di condotte reiterate e, comunque, quando le iniziative di carattere educativo adottate dall'istituzione scolastica non abbiano prodotto esito positivo, riferire alle autorità competenti;
- curare, attraverso le figure preposte, la realizzazione del curricolo di istituto di educazione civica affinché porti all'acquisizione delle competenze specifiche previste nel Profilo educativo, culturale e professionale dello studente a conclusione del primo e del secondo ciclo.

Hate speech: che cos'è e come prevenirlo

Il fenomeno di "incitamento all'odio" o "discorso d'odio" indica discorsi (post, immagini, commenti, ecc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificata come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente a catena. Più ampiamente, il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno è purtroppo sempre più diffuso ed è estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;

- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

Eventuali azioni volte a prevenire episodi di hate speech vengono integrate nell'attività didattica quotidiana attraverso lezioni sull'empatia, la diversità e l'inclusione che sensibilizzano sulla corretta comunicazione e sul corretto uso delle parole. Durante gli incontri di prevenzione al cyberbullismo verranno trattate, in modo più o meno approfondito, le dinamiche sopracitate (in base alle necessità della classe in cui verranno svolte le attività).

Dipendenza da Internet e gioco online

La dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della rete. L'Istituto, tramite gli incontri organizzati dalla Commissione Cyberbullismo, promuove percorsi sul benessere digitale.

Sexting

Il "sexting" è fra i rischi più diffusi connessi a un uso poco consapevole della rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti mediali sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze emotivamente impattanti per i protagonisti delle immagini, delle foto e dei video.

Adescamento online (grooming)

Il grooming (dall'inglese "to groom" – curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre bambini e/o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat (anche quelle interne ai giochi online), i social network in generale, le varie app di instant messaging (WhatsApp, Telegram, ecc.), i siti e le app di teen dating (siti di incontri per adolescenti). Un'eventuale relazione

sessuale può avvenire attraverso webcam o live streaming e portare anche a incontri dal vivo. In questi casi si parla di adescamento o grooming online.

In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies c.p. – adescamento di minorenni), quando è stata ratificata la Convenzione di Lanzarote (Legge 172 del 1° ottobre 2012). Tale problematica viene affrontata nel nostro Istituto nell'ambito di progetti legati all'educazione all'affettività.

Per riconoscere un eventuale caso di adescamento online è importante prestare attenzione a piccoli segnali che possono essere indicatori importanti, come ad esempio un cambiamento improvviso nel comportamento di un minore. A seguire, alcuni segnali e domande che potrebbero essere di aiuto:

- *Il minore ha conoscenze sessuali non adeguate alla sua età?*
- *Venite a conoscenza di un certo video o di una foto che circola online o che il minore ha ricevuto o filmato, ma c'è imbarazzo e preoccupazione nel raccontarvi di più?*
- *Il minore si isola totalmente e sembra preso solo da una relazione online?*
- *Ci sono prese in giro e allusioni sessuali verso un bambino/ragazzo in particolare?*

Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore, che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e della sessualità.

Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere all'adescatore. È importante che il computer o gli altri dispositivi elettronici del minore vittima non vengano usati, per non compromettere eventuali prove.

I casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni, a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad

esempio salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video).

L'adescamento, inoltre, può essere una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi a un servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico. Nei casi più estremi, in cui l'adescamento porta a un incontro fisico e a un abuso sessuale, un sostegno psicologico esperto per il minore è da considerarsi prioritario e urgente.

Pedopornografia

La pedopornografia online è un reato (art. 600-ter, comma 3, c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e e ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, concreti o simulati, o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

La Legge n. 269 del 3 agosto 1998 "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù" introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella Legge n. 38 del 6 febbraio 2006 "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet", segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600-ter e 600-quater c.p.), che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e e adolescenti realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Secondo la Legge 172/2012 – Ratifica della Convenzione di Lanzarote (art. 4), per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato: occorre parlarne sempre in considerazione della maturità e della fascia d'età, selezionando il tipo di informazioni che si possono condividere. È tuttavia un fenomeno di cui si deve sapere di più ed è

utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting. Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico, promuovendo i servizi di Generazioni Connesse: qualora navigando in rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it, alla sezione "Segnala contenuti illegali" (Hotline).

Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e ad altri contenuti illegali o dannosi diffusi attraverso la rete. I due servizi messi a disposizione dal Safer Internet Centre sono il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children.

Il nostro piano d'azioni (4)

Azioni da sviluppare nell'anno scolastico 2025/2026

- Mettere a disposizione, attraverso i canali di comunicazione dell'Istituto, contenuti sui rischi online fruibili da studenti e famiglie.

Azioni da sviluppare nel triennio successivo

- Organizzare laboratori e/o percorsi di sensibilizzazione sull'educazione alla sessualità e all'affettività rivolti agli studenti e alle studentesse.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi online, rivolti agli/alle studenti/studentesse, con il coinvolgimento di esperti (psicologi, Polizia Postale, associazioni, Azzurro Academy, Generazioni Connesse, AIDA Cremona, Fondazione Cecchettin, docenti del Politecnico, docenti di giurisprudenza).
- Organizzare uno o più incontri informativi, anche in orario pomeridiano e online, per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali, integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti e delle studentesse.
- Utilizzare la **web radio d'Istituto** come strumento di sensibilizzazione sui rischi online (cyberbullismo, hate speech, disinformazione) e su temi di educazione civica digitale

(benessere digitale, rispetto delle diversità, uso dell'IA), attraverso la realizzazione di contenuti informativi e campagne di comunicazione rivolte alla comunità scolastica.

Capitolo 5 – Segnalazione e gestione dei casi

Cosa segnalare

Il personale docente del nostro Istituto, quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online, ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e la gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire). Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola.

Nelle procedure sono indicate le figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso, e le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico. Inoltre, la scuola individua le figure che costituiranno un team preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio (richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola. Tali procedure sono comunicate e condivise con l'intera comunità scolastica. Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola: la scuola è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news sul sito della scuola, durante i collegi docenti e attraverso tutti i canali maggiormente utili a un'efficace comunicazione.

A seguire, le problematiche a cui fanno riferimento le procedure allegate.

Cyberbullismo: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito dalla vittima?). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/dalle studenti/esse coinvolti/e (e quindi valutare se rivolgersi a un servizio deputato a offrire un supporto psicologico e/o di mediazione).

Adescamento online: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne; inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando quindi di rispondere all'adescatore al suo posto. È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. L'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

Sexting: nel caso in cui immagini e/o video, anche prodotti autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffusi senza il loro consenso, è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online, e il blocco della sua diffusione via dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità sul minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi in rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Si suggeriscono, inoltre, i seguenti servizi: il servizio di Helpline 1.96.96 e la chat di Telefono Azzurro per supporto ed emergenze; Clicca e Segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale, in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni e alla

verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative. Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero presentare due casi:

- **Caso A (sospetto)**: il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.
- **Caso B (evidenza)**: il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

Per tutti i dettagli si faccia riferimento agli allegati con le procedure.

Strumenti a disposizione di studenti e studentesse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola prevede alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- scatola/box per la raccolta di segnalazioni anonime, da collocare in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi ad altre figure, enti, istituzioni e servizi presenti sul territorio, qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola. Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di

Telefono Azzurro (1.96.96) è sempre attiva nell'offrire una guida competente e un supporto in tale percorso.

A seguire, i principali servizi e le agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **Comitato Regionale UNICEF**: laddove presente, su delega della Regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione e anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni**: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della rete che includono gli estremi del reato.
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi ambulatori specificamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico**: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime; segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovuti a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

Il nostro piano d'azioni (5)

Azioni da sviluppare nell'anno scolastico 2025/2026

- Diffondere le **procedure di segnalazione** a tutto il personale.
- Presentare agli studenti e alle famiglie gli **strumenti di segnalazione**: docente referente e contatto email epolicy@istitutostradivari.it; sportello di ascolto; box per segnalazioni anonime (Google Moduli).

- Costituire o formalizzare il **team di gestione dei casi**.
- Proporre e chiedere l'approvazione al Consiglio di Istituto e al Collegio Docenti delle procedure interne in caso di fenomeni di cyberbullismo, sexting e adescamento online. Una volta approvate, estenderle a tutta la comunità educante.

Azioni da sviluppare nel triennio successivo

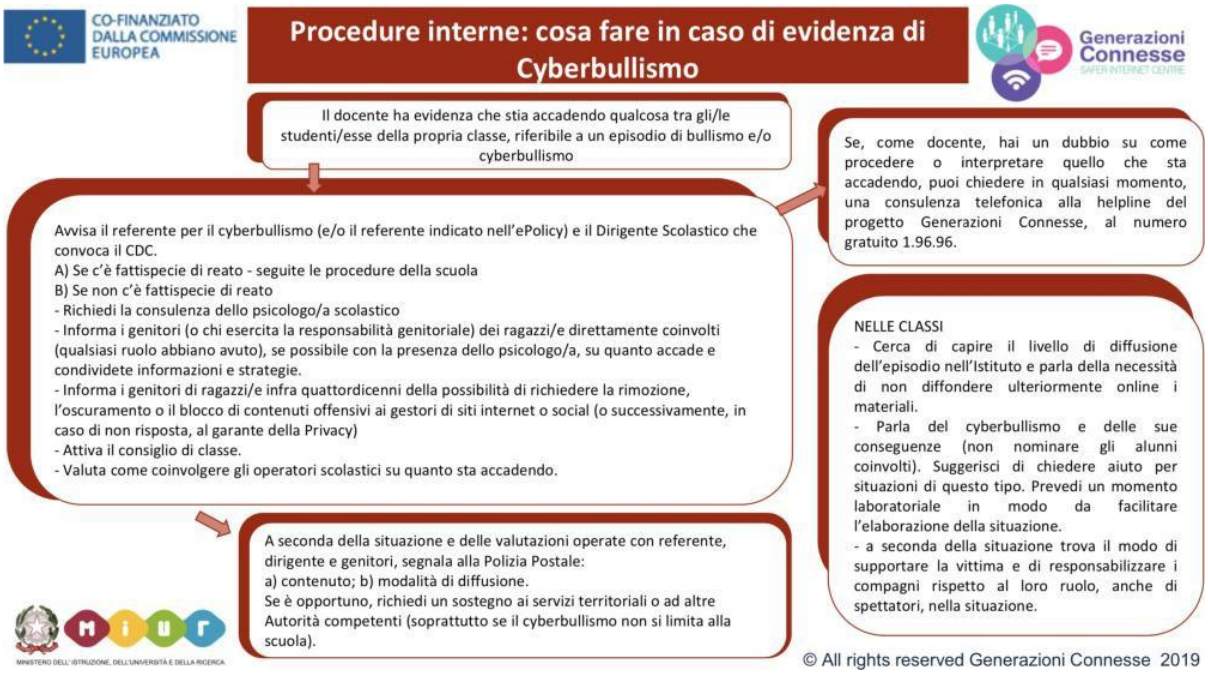
- Consolidare un **sistema strutturato di segnalazione**.
- Monitorare annualmente i casi e le tipologie di rischio.
- Costruire e condividere delle **FAQ** in base alle domande e segnalazioni più frequenti.
- Rafforzare la collaborazione con servizi territoriali, ASL e Polizia Postale.
- Valorizzare lo **sportello psicologico** anche in riferimento alle tematiche connesse.

Allegati: le procedure operative

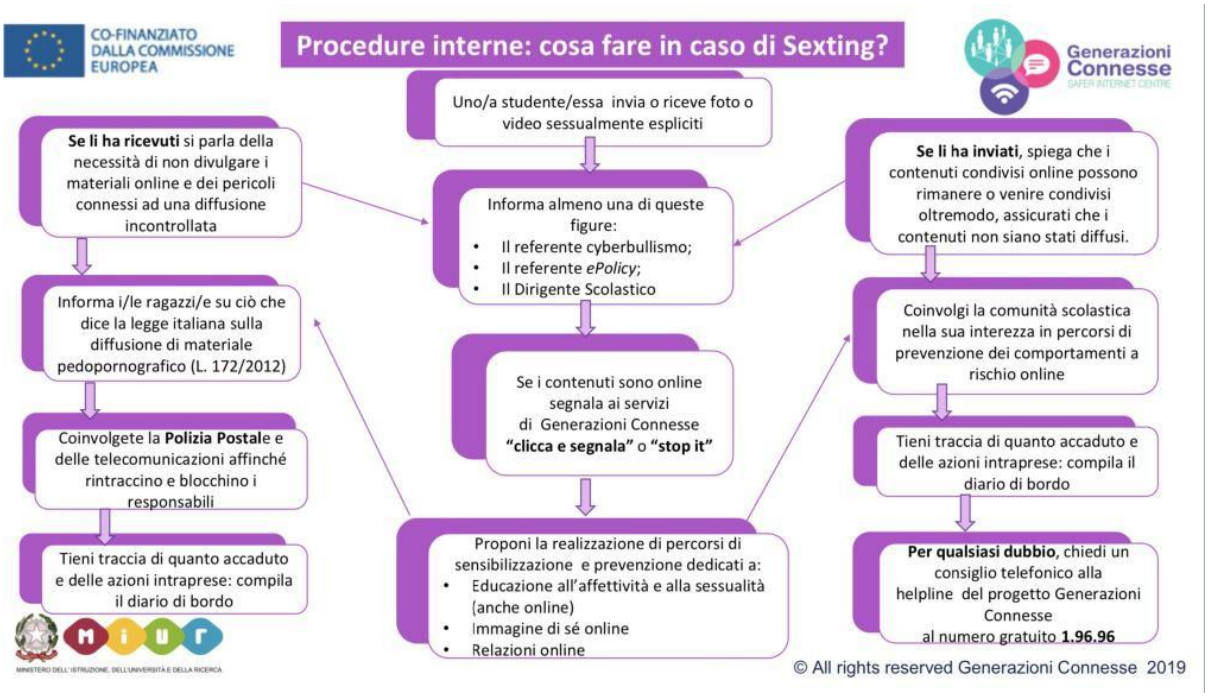
Si riportano di seguito le procedure operative di Generazioni Connesse adottate dall'Istituto.

Procedura: cosa fare in caso di sospetto di cyberbullismo

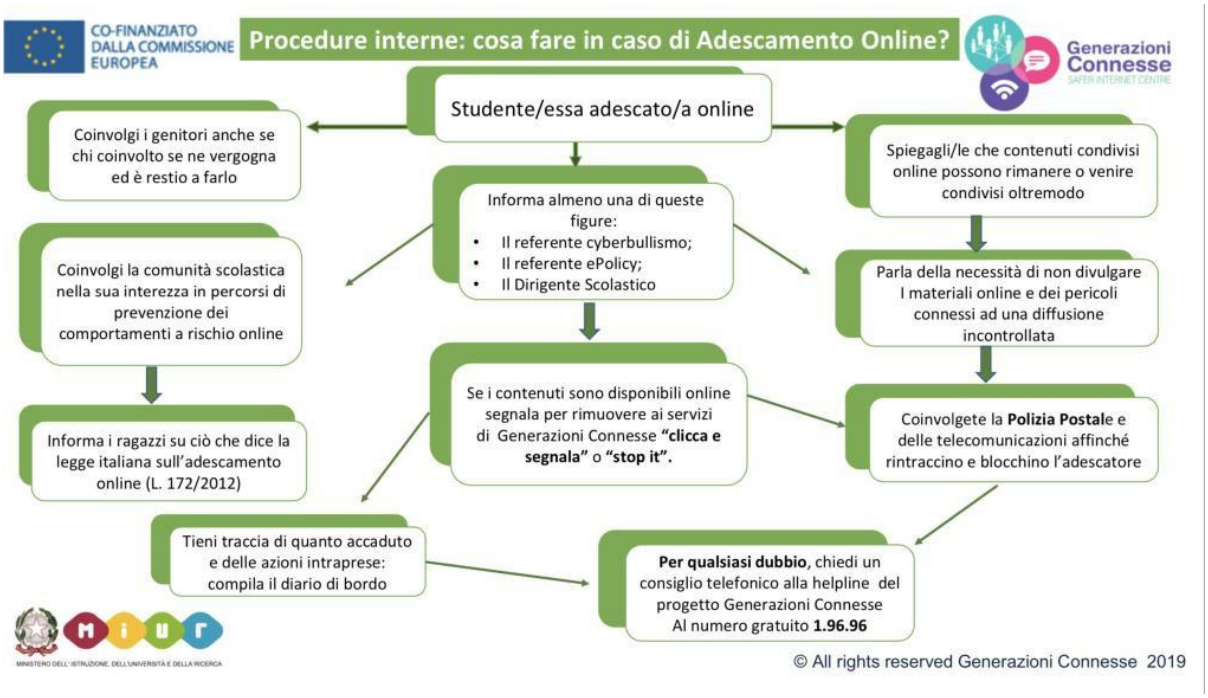
Procedura: cosa fare in caso di evidenza di cyberbullismo



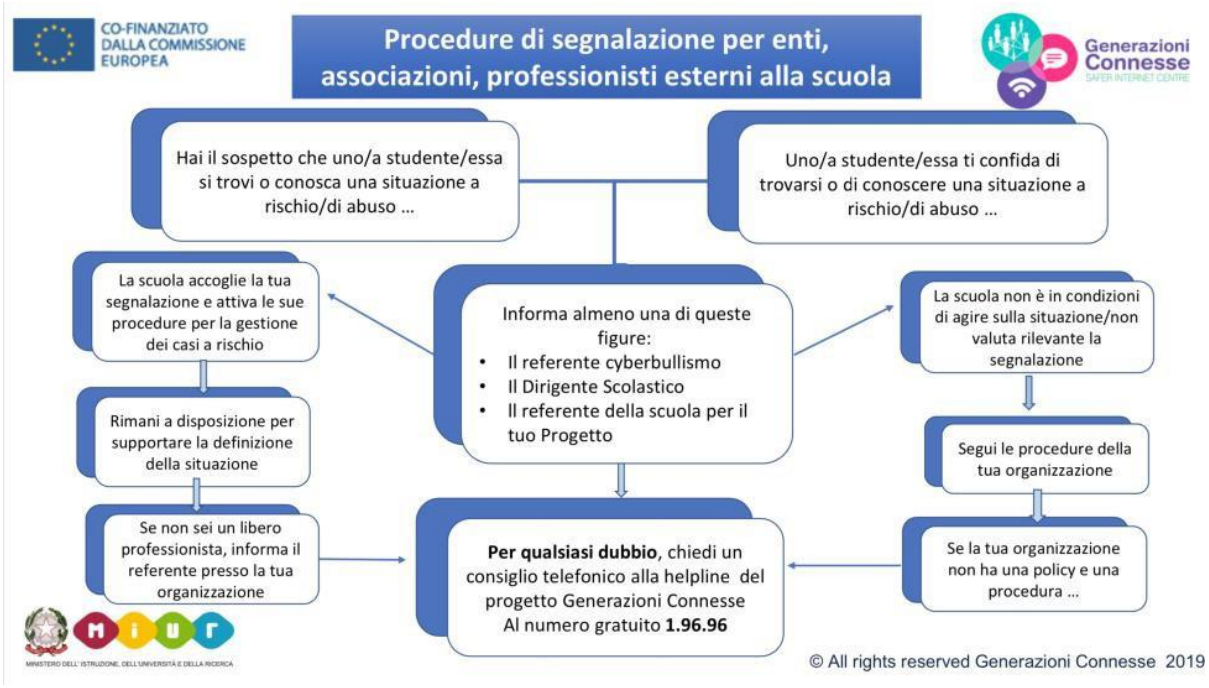
Procedura: cosa fare in caso di sexting



Procedura: cosa fare in caso di adescamento online



Procedura di segnalazione per enti, associazioni e professionisti esterni alla scuola



Altri allegati

- Scheda di segnalazione
- Diario di bordo
- iGloss@ 1.0 – l'ABC dei comportamenti devianti online
- Elenco dei reati procedibili d'ufficio.