

**CODICE DI INTERVENTO PER LA PREVENZIONE E IL
CONTRASTO DEI FENOMENI
DEL BULLISMO E DEL CYBERBULLISMO ed E-POLICY**
documento adottato
con delibera del Collegio dei Docenti n. 24 del 20 maggio 2025
e del Consiglio dell’Istituzione n. 34 del 17 giugno 2025

IC CIVEZZANO

1. INTRODUZIONE.....	1
1.1 SCOPO DEL PIANO DI INTERVENTO.....	1
1.2 RUOLI E RESPONSABILITÀ.....	1
1.3 QUADRO NORMATIVO DI RIFERIMENTO.....	3
1.4 TAVOLO PERMANENTE DI MONITORAGGIO.....	3
2. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI.....	4
2.1 PREVENZIONE.....	4
2.2 RILEVAZIONE.....	4
2.3 GESTIONE DEI CASI.....	5
3. E-POLICY.....	8
3.1 CURRICOLO E FORMAZIONE DOCENTI.....	8
3.2 SENSIBILIZZAZIONE DELLE FAMIGLIE.....	9
3.3 GESTIONE DELL’INFRASTRUTTURA E DELLA STRUMENTAZIONE DIGITALE DELLA SCUOLA.....	9
3.4 GESTIONE ACCESSI.....	10
3.5 E-MAIL, PIATTAFORME DIDATTICHE E APPLICAZIONI IN USO.....	10
3.6 SITO WEB DELLA SCUOLA.....	10
3.7. STRUMENTAZIONE PERSONALE.....	11
3.7.1 STUDENTI: GESTIONE DEI DISPOSITIVI PERSONALI.....	11
3.7.2 DOCENTI E PERSONALE DELLA SCUOLA: GESTIONE DEI DISPOSITIVI PERSONALI.....	11



1. INTRODUZIONE

1.1 SCOPO DEL PIANO DI INTERVENTO

Il fenomeno del bullismo e del cyberbullismo rappresenta una delle sfide più complesse e urgenti del nostro tempo, mettendo in pericolo il benessere, la sicurezza e lo sviluppo emotivo dei giovani. Per contrastare efficacemente questi comportamenti dannosi, è necessario adottare un approccio integrato e sistematico che unisca la sensibilizzazione, la prevenzione, l'intervento tempestivo e il supporto psicologico.

Nel contesto di tale impegno, il presente piano di intervento nasce dalla necessità di rispondere in modo concreto e coordinato alle modifiche normative introdotte dalla Legge 70/2017 e dalla Legge 71/2024. La Legge 70/2017 ha avuto un impatto significativo sul trattamento giuridico degli episodi di cyberbullismo, prevedendo misure specifiche per la protezione delle vittime e l'individuazione degli autori, con particolare attenzione all'ambito digitale. La Legge 71/2024, inoltre, ha esteso l'attenzione non solo al cyberbullismo, ma anche al fenomeno del bullismo, rafforzando le misure di prevenzione e d'intervento in ambito scolastico e promuovendo un approccio più ampio e integrato per combattere tutte le forme di violenza tra pari.

Il presente piano di intervento integra e assorbe la **policy e-safety** precedentemente adottata dall'istituto: mentre la policy e-safety ha gettato le basi per una gestione consapevole e sicura dell'uso delle tecnologie, questo documento amplia e rafforza le azioni già intraprese, rispondendo in modo più puntuale alle esigenze emergenti legate sia al cyberbullismo che al bullismo.

Il piano che segue, pertanto, integra le modifiche normative in un quadro unitario di azioni preventive, interventi rapidi, supporto psicologico e monitoraggio continuo, con l'obiettivo di garantire una risposta adeguata, tempestiva e duratura a fenomeni tanto gravi quanto diffusi.

1.2 RUOLI E RESPONSABILITÀ

Affinché il codice di intervento sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, si impegni nella sua attuazione e promozione.

Il **Dirigente Scolastico** si impegna per garantire la sicurezza, anche online, di tutti i membri della comunità scolastica. È formato adeguatamente sulla prevenzione di problematiche legate al bullismo e al cyberbullismo, in linea con il quadro normativo di riferimento. Promuove, insieme all'Animatore Digitale e al docente referente per il bullismo e il cyberbullismo, attività specifiche per tutte le figure scolastiche. Inoltre, il Dirigente ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo e cyberbullismo, collaborando con le Forze dell'ordine.

Il **Referente per il bullismo e il cyberbullismo** ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto di tali fenomeni. Si occupa della gestione delle eventuali segnalazioni di episodi di bullismo e cyberbullismo e, a tal fine, in accordo con il Dirigente scolastico, può collaborare con le Forze dell'ordine, le associazioni e i centri di aggregazione giovanile del territorio, coinvolgendoli, insieme a studenti, colleghi e genitori, in progetti e percorsi formativi dedicati.

L'**Animatore digitale** supporta il personale scolastico nelle attività legate al digitale ed è un punto di riferimento per la promozione di percorsi di formazione interna volti a sviluppare la "scuola digitale" e a favorire la consapevolezza e l'esercizio della cittadinanza digitale. Tali percorsi coinvolgono alunni, docenti e famiglie. Inoltre cura la sezione del sito dell'Istituto dedicata all'area digitale.

I Docenti hanno un ruolo centrale nel contrastare i fenomeni del bullismo e del cyberbullismo:

- sono tenuti a monitorare costantemente le dinamiche relazionali all'interno del gruppo classe e il comportamento del singolo alunno, mostrandosi disponibili all'ascolto e rilevando segnali di disagio o comportamenti a rischio;
- devono impegnarsi a prevenire qualsiasi forma di violenza tra pari, fisica, verbale o online, creando un ambiente in cui ogni studente possa sentirsi accolto e protetto. Inoltre, sono chiamati ad accompagnare e supportare gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso di dispositivi tecnologici che si connettono alla Rete;
- devono segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, sia fisico che digitale, che veda coinvolti studenti e studentesse, intervenendo tempestivamente per tutelare il benessere di tutti;
- sono tenuti a integrare nel curriculum della propria disciplina approfondimenti specifici che promuovano, oltre alla consapevolezza digitale, anche una cultura del rispetto, dell'inclusività e della responsabilità.

Il **personale Amministrativo, Tecnico e Ausiliario (ATA)** svolge funzioni miste, ossia di tipo amministrativo-contabile, tecniche e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il Dirigente scolastico e con il personale docente tutto.

Il personale ATA può essere coinvolto nelle attività di formazione e autoformazione in tema di bullismo e cyberbullismo; collabora nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure.

Il tecnico informatico a scuola svolge un ruolo cruciale per garantire il corretto funzionamento delle infrastrutture tecnologiche, la sicurezza dei sistemi e il supporto al personale e agli studenti. In particolare monitora e mantiene in efficienza la rete scolastica (LAN, Wi-Fi), garantendone la sicurezza, anche con l'installazione di antivirus, firewall e sistemi di filtraggio dei contenuti, in collaborazione con l'ufficio contabilità che cura gli acquisti di quanto necessario. Amministra l'accesso sicuro ai sistemi scolastici e alla GWS tramite login, password e autorizzazioni.

Gli **Studenti e le Studentesse** si impegnano, in relazione al proprio grado di maturità e consapevolezza raggiunta, a utilizzare al meglio gli strumenti e 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/le. Oltre a ciò, sono chiamati a sviluppare una consapevolezza critica riguardo ai comportamenti corretti e rispettosi da adottare anche nelle interazioni personali, contrastando attivamente il bullismo e promuovendo il rispetto reciproco nelle relazioni quotidiane. Devono partecipare attivamente a progetti e attività che riguardano l'uso positivo delle TIC e della Rete e la prevenzione dei fenomeni di bullismo e cyberbullismo. Sono tenuti a farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education, contribuendo così alla creazione di un ambiente scolastico basato sull'inclusione, sulla solidarietà e sul rispetto delle diversità. In questo modo, gli studenti e le studentesse svolgono un ruolo attivo nella costruzione di una cultura di rispetto che prevenga tutte le forme di violenza e discriminazione, sia fisiche che digitali.

I Genitori, in continuità con l'Istituto scolastico, potranno partecipare alle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali. Inoltre, sono chiamati a educare i propri figli e figlie al rispetto delle regole e al contrasto di qualsiasi forma di bullismo, sia online che offline, insegnando loro l'importanza del rispetto reciproco, della solidarietà e dell'inclusività, sia nel mondo digitale che nella vita quotidiana. I genitori hanno anche il dovere di relazionarsi in modo costruttivo con i docenti, nel rispetto di quanto previsto dal patto di corresponsabilità.



1.3 QUADRO NORMATIVO DI RIFERIMENTO

Il documento si inserisce all'interno di un quadro normativo più ampio. I principali riferimenti legislativi e regolamentari sono i seguenti:

A. Normative Europee

- Regolamento Generale sulla Protezione dei Dati (GDPR) - Regolamento UE 2016/679
Garantisce la protezione dei dati personali e stabilisce regole per il trattamento dei dati, con particolare attenzione alla tutela di bambini e adolescenti.

B. Normative Italiane

- Legge 71/2017 sul Cyberbullismo
Introduce disposizioni specifiche per la prevenzione e il contrasto del cyberbullismo, obbligando le scuole a:
 - Nominare un referente per il cyberbullismo.
 - Promuovere progetti di sensibilizzazione e prevenzione.
 - Collaborare con le autorità competenti in caso di episodi di bullismo o cyberbullismo.
- Legge 70/2024 – Disposizioni e delega al Governo in materia di prevenzione e contrasto del bullismo e del cyberbullismo
Modifica e integra la Legge 71/2017, rafforzando le misure rieducative ed educative in caso di condotte aggressive e di cyberbullismo da parte di minorenni. Prevede:
 - Percorsi di mediazione e rieducazione per i minori responsabili, coinvolgendo famiglie e servizi sociali.
 - Progetti educativi e riparativi che includono attività come laboratori creativi, sportivi o artistici per promuovere il rispetto e la comunicazione non violenta.
 - Interventi da parte del tribunale per i minorenni nei casi più gravi, con possibilità di affidamento ai servizi sociali o collocamento temporaneo in comunità.

C. Documenti provinciali:

- Codice di Comportamento dei Dipendenti della Provincia Autonoma di Trento ([Delibera della Giunta provinciale n. 1514 del 27 settembre 2024](#));
- Linee guida per il benessere digitale (Delibera [della Giunta provinciale](#) n. 1871 del 22/11/2024): include regole per un uso corretto delle risorse digitali in ambito scolastico, a tutela dell'efficacia del sistema educativo.

D. Integrazione del codice con Regolamenti Esistenti:

- il codice si integrerà con il Regolamento d'Istituto, il Progetto d'Istituto e il Patto di corresponsabilità già in vigore, armonizzandosi con questi documenti.

1.4 TAVOLO PERMANENTE DI MONITORAGGIO

Il Dirigente scolastico promuove, nell'ambito della propria autonomia, la costituzione di un tavolo permanente di monitoraggio per il contrasto dei fenomeni del bullismo e del cyberbullismo composto da rappresentanti degli insegnanti, delle famiglie ed eventuali esperti esterni, con la possibilità di invitare anche una rappresentanza di studenti.

Il tavolo presieduto dal Dirigente Scolastico (DS) si riunisce per:

1. monitorare e promuovere le azioni previste dal codice interno;
2. identificare aree di miglioramento nell'applicazione del codice e proporre iniziative formative o di sensibilizzazione per rafforzare i comportamenti positivi..

2. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

2.1 PREVENZIONE

La prevenzione e il contrasto del bullismo e del cyberbullismo rappresentano una priorità per ogni contesto educativo.

I docenti svolgono un ruolo fondamentale nel garantire un ambiente sicuro e rispettoso per tutti gli studenti. Attraverso azioni mirate, è possibile promuovere il benessere relazionale e prevenire episodi di prevaricazione o esclusione.

Di seguito sono riportate alcune strategie adottate per prevenire e affrontare efficacemente queste problematiche.

- **Promuovere la cultura del rispetto** – Integrare nei percorsi didattici attività che sensibilizzino gli studenti all’empatia, alla collaborazione e al rispetto reciproco, organizzare delle attività in occasione della Giornata del Rispetto (20 gennaio).
- **Monitorare le dinamiche di classe** – Osservare attentamente le relazioni tra gli studenti per individuare segnali di disagio o conflitti latenti e intervenire tempestivamente.
- **Creare spazi di dialogo e ascolto** – Organizzare momenti di confronto in cui gli alunni possano esprimere le proprie emozioni e difficoltà in un ambiente sicuro e accogliente.
- **Attivare uno sportello di ascolto** – Mettere a disposizione di alunni, genitori e insegnanti uno spazio di ascolto gestito dalla psicologa di Istituto.
- **Favorire la collaborazione con le famiglie** – Informare i genitori sull’importanza della prevenzione del bullismo e del cyberbullismo, fornendo strumenti utili per riconoscere e affrontare eventuali segnali di disagio nei figli.
- **Utilizzare il regolamento scolastico in modo chiaro e coerente** – Ricordare agli studenti le regole di convivenza e le conseguenze di eventuali comportamenti scorretti, garantendo un intervento tempestivo in caso di infrazioni.
- **Realizzare attività educative specifiche** – Organizzare incontri con esperti, percorsi specifici, progetti interdisciplinari e discussioni guidate per approfondire il tema del bullismo e del cyberbullismo e della consapevolezza in ambito digitale.
- **Favorire il lavoro cooperativo** – Incentivare il lavoro di gruppo e metodologie didattiche che rafforzino la collaborazione tra studenti, riducendo le dinamiche di esclusione e sopraffazione.
- **Promuovere attività di Peer education** – Promuovere progetti finalizzati alla formazione tra pari sui rischi connessi all’uso delle nuove tecnologie e la conoscenza dei reati correlati. Questo approccio educativo permette agli studenti di diventare protagonisti nella diffusione di informazioni e consapevolezza, rafforzando il loro senso di responsabilità e il loro ruolo attivo nella prevenzione.
- **Promuovere iniziative di formazione, tavoli di lavoro e momenti di confronto** dedicati a genitori e insegnanti sul tema dell’uso consapevole del digitale e sui rischi connessi alla navigazione in rete.

Per quanto riguarda la prevenzione del fenomeno del cyberbullismo vanno considerate anche le azioni riportate al punto 3. [E-POLICY](#).

2.2 RILEVAZIONE

La segnalazione di episodi problematici è un atto importante per prevenire situazioni di disagio.

Alla Scuola Primaria gli studenti che si trovano in situazioni di sofferenza o che assistono a episodi di bullismo e/o cyberbullismo possono segnalare quanto accaduto attraverso diverse modalità:

1. ai docenti di classe;
2. ai collaboratori scolastici;



3. ai genitori, i quali possono rivolgersi al docente coordinatore di classe, ai Referenti per il bullismo e il cyberbullismo o al Dirigente scolastico.

Alla Scuola Secondaria di Primo Grado gli studenti che si trovano in situazioni di disagio o che assistono a episodi di bullismo e/o cyberbullismo possono segnalare quanto accaduto attraverso diverse modalità:

1. ai docenti di classe;
2. ai collaboratori scolastici;
3. ai peer educator: gli studenti possono rivolgersi direttamente ai peer educator, che sono formati per accogliere e gestire con sensibilità le segnalazioni o inviare una mail all'indirizzo: peer.civezzano@iccivezzano.eu.
4. alla psicologa: inserendo una richiesta scritta nell'apposita bussola posta nel corridoio della sede scolastica;
5. al docente Referente per il bullismo e il cyberbullismo;
6. alla Dirigente scolastica.

Tutte le segnalazioni verranno gestite con la massima discrezione, rispettando la riservatezza delle persone coinvolte. L'obiettivo è quello di affrontare ogni caso con sensibilità e tempestività, garantendo un supporto adeguato sia alla vittima che ai testimoni.

Ecco alcuni esempi di comportamenti che devono essere segnalati:

1. Bullismo:
 - Insulti, minacce o offese ripetute nei confronti di uno studente.
 - Esclusione volontaria e ripetuta da attività o gruppi.
 - Aggressioni fisiche o psicologiche.
2. Cyberbullismo:
 - Messaggi offensivi o minatori inviati tramite social network, chat o email.
 - Diffusione di foto, video o informazioni personali senza il consenso dell'interessato.
 - Commenti o post denigratori sui social media.
3. Sexting:
 - Scambio di immagini o video a contenuto sessuale tramite smartphone o internet.
 - Condivisione non consensuale di contenuti intimi arrecando danno alla persona ritratta.
4. Adescamento online:
 - Tentativi di instaurare rapporti di fiducia da parte di adulti per sfruttare un minore.
 - Comportamenti sospetti o richieste inappropriate ricevute da estranei in rete.
5. Violazione della privacy:
 - Pubblicazione o condivisione di dati personali (indirizzo, numero di telefono, ecc.) senza il consenso dell'interessato.
 - Accesso non autorizzato ai profili social o ai dispositivi personali.

2.3 GESTIONE DEI CASI

La gestione dei casi di bullismo e cyberbullismo richiede un intervento strutturato e coordinato per garantire una risposta efficace e tempestiva.

Accogliere la segnalazione di un presunto caso di bullismo ha lo scopo di:

- attivare un processo di attenzione e di successive valutazioni;

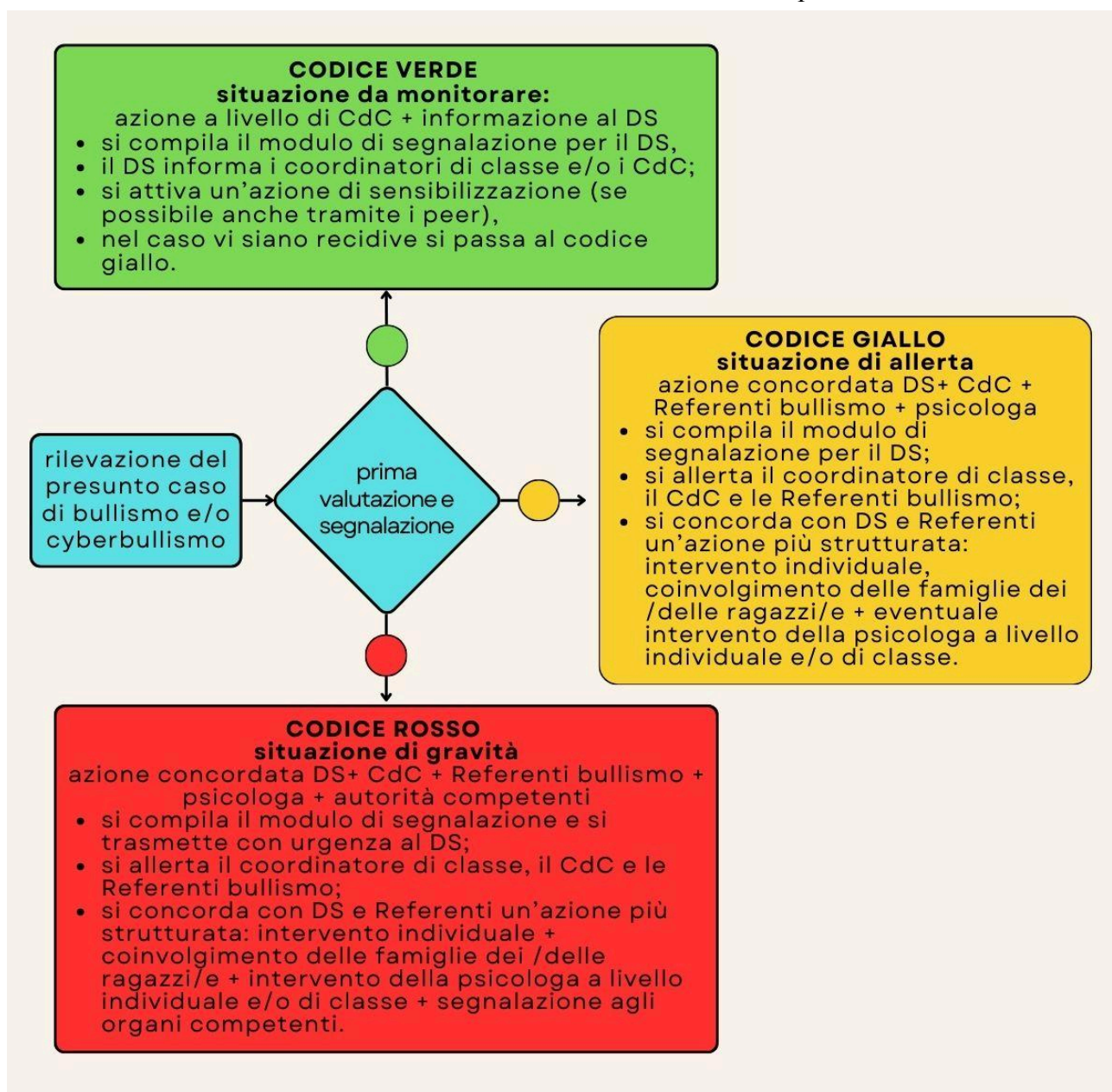
- attivare un processo di presa in carico di una situazione che deve essere valutata;
- escludere che un caso di sofferenza venga sottovalutato o ritenuto poco importante;

La prima segnalazione può essere fatta da chiunque: vittima, genitori, testimoni, docenti, personale ATA, ecc., utilizzando il modulo specificamente messo a disposizione di tutti ([allegato n. 1](#)), facendo attenzione alle strategie riportate alla pagina 2 del citato modulo.

Il modulo di segnalazione sarà portato all'attenzione del Dirigente Scolastico.

Se la situazione è stata inquadrata come "CODICE VERDE" la gestione avverrà a livello di Consiglio di Classe.

Nel caso in cui chi raccoglie la segnalazione ritenga ci si trovi davanti ad una situazione inquadrabile in un "CODICE GIALLO" o "CODICE ROSSO" si concordano azioni più strutturate.



STRATEGIE DA SEGUIRE PER LA GESTIONE DELLA SITUAZIONE A RISCHIO

Intervento con la vittima	Intervento con il presunto bullo
<ul style="list-style-type: none"> - accogliere la vittima in un luogo tranquillo e riservato; - mostrare supporto alla vittima non colpevolizzarla per ciò che è successo; - far comprendere che la scuola è motivata ad aiutare e sostenere la vittima; - informare progressivamente la vittima su ciò che accade di volta in volta; - concordare appuntamenti successivi (per monitorare la situazione e raccogliere ulteriori dettagli utili). 	<ul style="list-style-type: none"> - è importante, prima di incontrarlo, essere al corrente di cosa è accaduto; - accogliere il presunto bullo in una stanza tranquilla, non accennare prima al motivo del colloquio; - iniziare il colloquio affermando che si è al corrente dello specifico episodio offensivo di prevaricazione; - fornire al ragazzo/a l'opportunità di esprimersi, favorire la sua versione dei fatti; - mettere il presunto bullo di fronte alla gravità della situazione; - non entrare in discussioni; - cercare insieme possibili soluzioni ai comportamenti prevaricatori; - ottenere, quanto più possibile, che il presunto bullo dimostri comprensione del problema e bisogno di riparazione; - in caso di più bulli, i colloqui avvengono preferibilmente in modo individuale con ognuno di loro, uno di seguito all'altro, in modo che non vi sia la possibilità di incontrarsi e parlarsi; - una volta che tutti i bulli sono stati ascoltati, si procede al colloquio di gruppo.
	Colloquio di gruppo con i presunti bulli
	<ul style="list-style-type: none"> - iniziare il confronto riportando quello che è emerso dai colloqui individuali; - l'obiettivo è far cessare le prevaricazioni individuando soluzioni positive.
<p><i>Far incontrare prevaricatore e vittima - questa procedura può essere adottata solo se le parti sono pronte e il Team rileva un genuino senso di pentimento e di riparazione nei prepotenti;</i></p> <p>è importante:</p> <ul style="list-style-type: none"> - ripercorrere l'accaduto lasciando la parola al bullo/i; - ascoltare il vissuto della vittima circa la situazione attuale; - condividere le soluzioni positive e predisporre un piano concreto di cambiamento 	
<p>Coinvolgimento del gruppo classe o di possibili spettatori: questa azione si consiglia solo quando possiamo rilevare un chiaro segnale di cambiamento nel presunto/i bullo/i e il coinvolgimento del gruppo non implica esposizioni negative della vittima, ma può facilitare la ricostruzione di un clima e di relazioni positive.¹</p>	

¹ tabella tratta dalle “Linee di orientamento per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo”, emanate dal Ministero dell’Istruzione (13 gennaio 2021)



Il modulo di segnalazione sarà portato sempre all'attenzione del Dirigente Scolastico. Una volta valutata e inquadrata la situazione in una delle tre fasce di livello (codice verde, giallo o rosso) si procederà con le azioni previste.

Gli episodi inquadrati come codice verde saranno gestiti a livello di Consiglio di classe.

Per i fenomeni riconosciuti come codice giallo o rosso, il Dirigente scolastico in collaborazione con il **Team Antibullismo**, composto dalle Referenti bullismo e cyberbullismo, integrato dai coordinatori delle classi coinvolte ed eventualmente dalla Psicologa di Istituto di riferimento, raccolte le informazioni necessarie, valuterà quali azioni mettere in campo.

A titolo esemplificativo si riportano alcune delle possibili strategie da adottare:

1. convocazione dei genitori: i genitori degli alunni coinvolti potranno essere convocati per un colloquio. Durante l'incontro, verranno condivise informazioni sul caso e sulle possibili azioni educative da intraprendere;
2. coinvolgimento della psicologa dell'istituto: nei casi più complessi, verrà richiesto l'intervento della psicologa scolastica per fornire supporto psicologico agli studenti coinvolti. Potranno, inoltre, essere attivati percorsi di ascolto e mediazione, mirati a risolvere il conflitto e favorire la consapevolezza delle conseguenze delle azioni;
3. adozione di azioni educative che vedano protagonisti gli studenti coinvolti;
4. richiesta di supporto alla helpline di Generazioni Connesse (tel. 1.96.96): questa linea di aiuto offre consulenza su come gestire episodi di cyberbullismo e problemi legati all'uso delle tecnologie digitali;
5. segnalazione al Team territoriale per l'Emergenza (se presente) e/o alle forze dell'ordine: nei casi di maggiore gravità (minacce gravi, diffusione di contenuti illeciti, adescamento, violazioni della privacy), il caso sarà segnalato alle autorità competenti, quali Polizia Postale o Carabinieri. Le segnalazioni saranno effettuate in conformità alla normativa vigente e coinvolgendo i genitori degli alunni interessati.

Tutti gli interventi saranno documentati e monitorati per garantire un follow-up adeguato e il supporto continuo agli studenti coinvolti.

L'obiettivo principale nella gestione di eventuali episodi o potenziali situazioni di rischio è educativo: non solo correggere i comportamenti scorretti, ma anche promuovere nei ragazzi una maggiore consapevolezza delle proprie azioni e delle loro conseguenze, valorizzando il dialogo attivo come strumento di comprensione e cambiamento.

3. E-POLICY

3.1 CURRICOLO E FORMAZIONE DOCENTI

Il collegio dei docenti dell'IC Civezzano con Deliberazione n. 16 del 28 febbraio 2024 ha adottato e fatto proprio il curriculum digitale <https://curriculum-digitale.iprase.tn.it/>, validato scientificamente dall'IPRASE.

La scuola, al fine di promuovere un utilizzo consapevole, sicuro ed efficace delle Tecnologie nella didattica, organizza specifici percorsi di formazione rivolti ai docenti e al personale scolastico.

Periodicamente vengono attivati corsi dedicati all'integrazione degli strumenti tecnologici e delle piattaforme digitali nei processi di insegnamento e apprendimento. Questi percorsi, condotti da esperti interni ed esterni, forniranno competenze pratiche e metodologiche su:

- utilizzo di software e applicazioni educative;
- gestione di piattaforme per la didattica digitale;
- creazione e condivisione di contenuti;
- strategie innovative per la didattica digitale e interattiva;



- inclusione e accessibilità attraverso le tecnologie.

Parallelamente, la scuola promuoverà percorsi di sensibilizzazione e approfondimento sui rischi legati all'uso dei dispositivi digitali, con particolare attenzione alla prevenzione e il contrasto del cyberbullismo e ai rischi della dipendenza da internet e dai social media.

Questi percorsi formativi mirano a dotare il personale scolastico di strumenti operativi e conoscenze adeguate per favorire un ambiente di apprendimento sicuro e innovativo, capace di valorizzare le potenzialità delle tecnologie riducendo al minimo i rischi.

3.2 SENSIBILIZZAZIONE DELLE FAMIGLIE

La scuola, per sensibilizzare le famiglie, organizza incontri informativi per:

- accrescere le conoscenze sull'uso della tecnologia e dei rischi ad essa connessi;
- fornire strategie per la gestione dei contenuti e degli strumenti digitali;
- approfondire le responsabilità degli studenti e dei genitori connesse ad un uso scorretto degli strumenti tecnologici;
- illustrare il curriculum sulle competenze digitali e/o il contenuto del codice di intervento per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo

L'Istituto promuove la creazione di accordi condivisi tra famiglie, scuola ed enti educativi per accompagnare bambini e adolescenti nell'uso consapevole della tecnologia.

Sul sito istituzionale, all'interno dell'area dedicata al digitale, è presente una sezione specifica rivolta ai genitori, pensata per offrire supporto nella gestione quotidiana della tecnologia in ambito familiare, valorizzandone al contempo i benefici. Sono disponibili suggerimenti pratici per definire regole di utilizzo dei dispositivi digitali, gestire in modo equilibrato il tempo trascorso davanti agli schermi e monitorare le attività online, con l'obiettivo di garantire ai bambini e ai ragazzi un'esperienza digitale sicura e protetta.

Inoltre, vengono trattati temi importanti come la privacy online, i pericoli della rete e come utilizzare al meglio le risorse digitali per l'apprendimento.

3.3 GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE DIGITALE DELLA SCUOLA

Per garantire un accesso sicuro e controllato a internet all'interno della scuola, abbiamo adottato diverse misure di protezione e monitoraggio.

La scuola ha aderito al servizio di URL filtering offerto da TNDIGITALE, che consente di filtrare i contenuti web e limitare l'accesso a siti non appropriati, proteggendo così studenti e docenti da rischi legati alla navigazione online.

I notebook e i computer fissi utilizzati nelle attività didattiche sono collegati alle lavagne interattive e accedono a internet tramite rete LAN o Wi-Fi, garantendo una connessione stabile e sicura.

Per quanto riguarda la protezione da minacce informatiche, tutti i dispositivi sono dotati di Microsoft Defender, il sistema antivirus dedicato che offre protezione in tempo reale contro malware e altre minacce. Inoltre, sul server in cloud è installato Trend Micro, una soluzione avanzata per la sicurezza informatica, che contribuisce a proteggere i dati e le infrastrutture scolastiche.

Un'ulteriore misura di controllo è stata implementata presso l'aula Tecnolab della SSPG di Civezzano, dove sulla postazione docente è attivo il software Veyon. Questo strumento permette di monitorare e gestire 21 dispositivi, offrendo la possibilità di supervisionare l'attività degli studenti durante le esercitazioni e di supportare nell'uso delle tecnologie digitali in modo sicuro ed efficace.

Grazie a queste soluzioni, la scuola si impegna a garantire un ambiente digitale protetto, promuovendo al contempo un uso responsabile e consapevole delle tecnologie.



3.4 GESTIONE ACCESSI

I computer dell'Istituto richiedono l'inserimento di credenziali per l'accesso, in quanto sono integrati in un dominio scolastico.

Le credenziali del personale docente e degli studenti della Scuola Secondaria di Primo Grado (SSPG) sono individuali, mentre alla Scuola Primaria, per facilitare l'accesso, vengono utilizzati account di classe.

Sono inoltre previsti alcuni account guest (ospite) destinati ai visitatori esterni o ai supplenti con contratto a breve termine.

Ogni utente è tenuto a non condividere le proprie credenziali/password con nessuno. In caso di compromissione o smarrimento della password, è necessario notificarlo immediatamente alla segreteria o al tecnico informatico.

Per garantire un utilizzo sicuro dei dispositivi e dei servizi informatici, l'Istituto:

- stabilisce che nessuno deve accedere ai dispositivi e ai servizi utilizzando credenziali altrui;
- richiede che tutti gli utenti si disconnettano al termine della sessione di lavoro o quando devono lasciare il computer incustodito;
- invita a non utilizzare sessioni lasciate aperte per errore da altri utenti: in questi casi è obbligatorio effettuare il logout e informare l'utente interessato;
- mantiene le attrezzature in condizioni di sicurezza.

3.5 E-MAIL, PIATTAFORME DIDATTICHE E APPLICAZIONI IN USO

Ciascuno studente e docente è dotato di una mail @iccivezzano.eu collegata alla Google Workspace di Istituto.

Per motivi di sicurezza la casella di posta elettronica degli studenti @iccivezzano.eu non potrà inviare o ricevere mail da persone esterne alla GWS di Istituto.

I docenti per facilitare la diffusione dei materiali e la gestione delle attività potranno utilizzare "Classroom" o cartelle condivise dedicate.

La Segreteria e la Dirigenza inviano le comunicazioni istituzionali alle famiglie e ai docenti principalmente attraverso il Registro Elettronico ISI-REL. L'utilizzo della mail rimane comunque un canale utilizzato seppur in via residuale o secondario.

3.6 SITO WEB DELLA SCUOLA

La scuola è dotata di un sito istituzionale conforme alle Linee Guida sull'accessibilità degli strumenti informatici emanate dall'AGID.

Il sito ufficiale dell'Istituto Comprensivo è accessibile all'indirizzo <http://www.iccivezzano.eu/> e rappresenta uno strumento fondamentale di comunicazione tra la scuola, le famiglie, il personale scolastico e il territorio.

La gestione del sito web è affidata all'**Animatore Digitale** e al personale di **Segreteria**, che ne curano l'aggiornamento e la manutenzione attraverso il pannello di amministrazione. È loro responsabilità garantire che i contenuti pubblicati siano accurati, aggiornati e conformi alla normativa sulla privacy e sulla trasparenza amministrativa.

Sul sito è possibile trovare:

- regolamenti e documenti ufficiali della scuola;
- pubblicazione di atti e comunicazioni istituzionali;
- procedure amministrative e didattiche;
- informazioni dettagliate sui servizi offerti dalla scuola;
- documentazione relativa ad attività curricolari ed extracurricolari;
- eventi, progetti e iniziative rivolte agli studenti e alle famiglie.

I docenti possono accedere a una **sezione riservata** del sito, dedicata alla condivisione di



comunicazioni interne e documentazione relativa all'organizzazione scolastica, come:

- circolari e avvisi interni;
- materiali di supporto alla didattica;
- calendari di riunioni e attività scolastiche;
- modulistica e procedure operative.

L'accesso a questa area non è nominativo: è stata creata un'unica credenziale condivisa tra tutti i docenti. Gli utenti sono tenuti a non divulgare le credenziali di accesso a persone non autorizzate e a utilizzarle esclusivamente per finalità istituzionali.

3.7. STRUMENTAZIONE PERSONALE

3.7.1 STUDENTI: GESTIONE DEI DISPOSITIVI PERSONALI

L'uso degli smartphone, degli smartwatch o di altri dispositivi rimane vietato durante l'orario scolastico, come previsto dal Regolamento di Istituto (art. 14 bis).

La scuola promuove l'utilizzo consapevole e guidato di dispositivi di proprietà della scuola, come tablet e computer portatili a fini didattici. L'uso di tali strumenti deve essere conforme alle normative vigenti in materia di protezione dei dati personali (Regolamento UE 2016/679 - GDPR). In particolare:

- l'accesso a risorse didattiche online è consentito solo attraverso reti sicure e con l'adozione di misure di sicurezza adeguate per la protezione dei dati personali degli studenti.
- è vietata la registrazione di immagini, audio o video di persone senza autorizzazione preventiva, salvo progetti specifici approvati dalla scuola e con consenso informato di genitori o tutori.

3.7.2 DOCENTI E PERSONALE DELLA SCUOLA: GESTIONE DEI DISPOSITIVI PERSONALI

L'utilizzo di dispositivi di proprietà da parte del personale docente e non docente durante l'orario scolastico deve avvenire esclusivamente per scopi lavorativi e in conformità con i principi di etica e responsabilità professionale.

È richiesto che:

- I dispositivi personali utilizzati per attività didattiche o amministrative siano protetti da password sicure.
- Non vengano salvati dati personali o sensibili degli studenti su dispositivi personali, salvo approvazione del Dirigente Scolastico e previa adozione di misure adeguate alla loro protezione.
- Si evitino pratiche di condivisione di file o informazioni personali tramite canali non ufficiali.

La scuola incoraggia inoltre l'uso di strumenti messi a disposizione dall'istituto (es. computer o tablet scolastici) per garantire un controllo adeguato e la conformità alle normative sulla privacy e sulla sicurezza digitale.