MINISTERO DELL'ISTRUZIONE E DEL MERITO

Liceo Scientifico Linguistico Statale "Paolo Giovio"

REGOLAMENTO E-POLICY
ai sensi della legge 17 maggio 2024, n. 70 recante "Disposizioni e delega al Governo in materia di prevenzione e contrasto del bullismo e del cyberbullismo"

INDICE

Introduzione
Scopo della Policy.
Ruoli e Responsabilità (*che cosa ci si aspetta da tutti gli attori della Comunità Scolastica*). Condivisione e comunicazione della Policy all'intera comunità scolastica.
Gestione delle infrazioni alla Policy.
Monitoraggio dell'implementazione della Policy e suo aggiornamento.

Formazione
Curricolo sulle competenze digitali per gli studenti.
Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica.
Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
Sensibilizzazione delle famiglie.

Gestione dell'infrastruttura e della strumentazione ICT della scuola.
Accesso ad Internet: filtri antivirus e sulla navigazione.
Gestione accessi (password, backup, ecc.).
Sito web della scuola Social network.
Protezione dei dati personali.

Strumentazione personale
Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc..
Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc..
Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc..

Prevenzione, rilevazione e gestione dei casi
Prevenzione
Rischi
Azioni
Rilevazione
Che cosa segnalare
Come segnalare: quali strumenti e a chi. Come gestire le segnalazioni.
Gestione dei casi

Definizione delle azioni da intraprendere a seconda della specifica del caso.

Introduzione

Scopo della e-Safety Policy

Scopo della e-Safety Policy è quello di stabilire i principi che regolano l'uso corretto e responsabile delle apparecchiature elettroniche nell'ambito dell'attività scolastica (e extrascolastica) nel rispetto della normativa vigente.
Le apparecchiature presenti nella Scuola sono un patrimonio comune, pertanto, vanno utilizzate con il massimo rispetto. Il loro utilizzo è regolamentato da criteri che puntano a ottimizzarne la gestione e la fruibilità: le prenotazioni, la tracciabilità dell'uso dei dispositivi informatici, la segnalazione di malfunzionamenti sono accorgimenti necessari per evitare disguidi organizzativi, smarrimenti e individuare un uso inappropriato o la causa di un danno.
Gli insegnanti sono responsabili della dotazione informatica nell'ambito dell'attività didattica e hanno il compito di rendere gli alunni consapevoli dell'importanza di salvaguardare questo bene comune, seguendo le corrette norme di utilizzo.
Con questo documento ci si propone: di salvaguardare gli studenti dell'Istituto e tutto il personale scolastico; di creare le condizioni per lavorare in modo sicuro e responsabile; di rendere gli utenti pienamente consapevoli dei rischi a cui si espongono quando navigano in rete; di impostare codici di condotta chiari e condivisi relativamente all'uso di internet per scopo didattico, personale o ricreativo; di affrontare gli abusi online e garantire che tutti i membri della comunità scolastica siano a conoscenza del fatto che comportamenti illeciti o pericolosi non sono accettabili e che verranno sanzionati.

Aree di rischio individuabili per la nostra comunità scolastica:

esposizione a contenuti inappropriati visita di siti web inappropriati validazione di informazioni e contenuti grooming (adescamento online)
sexting (condivisione di testi o immagini sessualmente esplicite) bullismo online
furto di identità reputazione online
salute e benessere (quantità di tempo passato davanti a diversi dispositivi) copyright (mancata considerazione dei diritti d'autore soprattutto per musica e film)

Ruoli e responsabilità

RUOLO	RESPONSABILITA'
Dirigente Scolastico	Garantire la sicurezza e l'integrità dei dati; Garantire che la scuola utilizzi un Internet Service filtrato approvato, conforme ai requisiti di legge vigenti; Assicurare che il personale riceva una formazione adeguata per svolgere i ruoli di sicurezza online Conoscere i protocolli da seguire in caso di infrazione della e-Policy Revisionare la e-Policy Ricevere relazioni di monitoraggio periodiche della sicurezza online da parte del responsabile.
Referente antibullismo e anticyberbullismo e team anti bullismo e anti cyberbullismo per la gestione delle emergenze)	Promuovere la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica Assicurare che l'educazione alla sicurezza online sia integrata nella consueta attività didattica; Garantire che tutto il personale sia a conoscenza dei protocolli da seguire in caso di incidente per la sicurezza online; Garantire che sia tenuto un registro degli incidenti di sicurezza online; Facilitare la formazione e la consulenza per tutto il personale; Coinvolgere enti esterni in attività formative rivolte agli alunni, alle famiglie, al personale docente. Controllare la condivisione di dati personali; Controllare l'accesso a materiali illegali o inadeguati; Controllare probabili azioni di cyberbullismo. Predisporre un modello per la segnalazione. Adozione di un protocollo per le emergenze.
Insegnanti	Inserire tematiche legate alla sicurezza online nell'attività didattica Supervisionare e guidare gli alunni quando lavorano impiegando apparecchiature elettroniche e la rete internet; Garantire che gli alunni siano consapevoli dei potenziali rischi e dei comportamenti impropri connessi alle attività online; Non salvare sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili; Non allontanarsi dalla postazione lasciandola incustodita, se non prima di aver effettuato la disconnessione; Segnalare prontamente eventuali malfunzionamenti o danneggiamenti al tecnico informatico;

Personale scolastico	Comprendere e contribuire a promuovere politiche di sicurezza online; Essere consapevoli dei problemi di sicurezza connessi all'uso di telefoni cellulari, fotocamere e dispositivi portatili; Attuare comportamenti sicuri, responsabili e professionali nell'uso delle apparecchiature elettroniche; Garantire che le comunicazioni con gli studenti avvengano in modo professionale e solo attraverso i canali impiegati dalla scuola. Monitorare l'utilizzo di dispositivi elettronici; Segnalare qualsiasi abuso o problema ai responsabili della sicurezza online
Studenti	Leggere, comprendere e accettare la e-Policy; Comprendere e essere consapevoli dei potenziali rischi e dei comportamenti impropri connessi alle attività online; Capire l'importanza di segnalare gli abusi e l'uso improprio di apparecchiature elettroniche o l'accesso a materiali inappropriati; Conoscere e capire la politica d'Istituto relativa all'uso di cellulari, computer, tablet e fotocamere; Conoscere e capire la politica della scuola sull'uso delle immagini e il cyberbullismo; Non utilizzare la strumentazione della scuola a scopi personali, ludici e/o ricreativi (a meno che l'attività didattica non lo preveda esplicitamente); Non eseguire tentativi di modifica della configurazione di sistema delle macchine Non utilizzare propri dispositivi esterni personali senza aver acquisito il permesso da parte dell'insegnante; Chiudere correttamente la propria sessione di lavoro. Capire l'importanza di adottare buone pratiche di sicurezza online quando si usano apparecchiature elettroniche, anche fuori dalla scuola;
Genitori	Sostenere la scuola nel promuovere la sicurezza online; Leggere, comprendere e controfirmare il patto di corresponsabilità; Accedere al sito della scuola in conformità con quanto stabilito dalla e-Policy; Controllare i dispositivi dei propri figli accertandosi che non vengano utilizzati per visualizzare, scaricare, creare e condividere contenuti inappropriati o pericolosi. Evitare ogni comportamento online che possa compromettere una corretta e rispettosa comunicazione fra i vari soggetti della comunità scolastica.

Al fine di garantire una gestione corretta, la scuola attua le seguenti strategie

Il Dirigente Scolastico si riserva, sentiti i responsabili, di limitare l'accesso alla rete internet attraverso i normali dispositivi di protezione presenti nei sistemi operativi.

Si attrezza per evitare comportamenti che non rientrano nelle norme approvate da Collegio Docenti in merito a tali comportamenti:

- scaricare file protetti da copyright;
- visitare siti non adatti alla normale attività didattica;
- utilizzare la rete per scopi privati e personali che non hanno attinenza con l'attività didattica;
- alterare i parametri di protezione dei computer in uso a scuola.

Disposizioni, comportamenti, procedure:

Il sistema informatico è periodicamente controllato dai responsabili (Amministratore di Sistema, AA.TT., A.D.);

La scuola può controllare i file utilizzati, i file temporanei e siti visitati da ogni macchina; E' vietato installare e scaricare da Internet software non autorizzati;

Verifiche antivirus vengono condotte periodicamente sui computer;

L'utilizzo di CD e chiavi USB personali deve essere utilizzato previa scansioni antivirus;

Il materiale didattico dei docenti può essere messo in rete sempre nell'ambito del presente regolamento e nel rispetto delle leggi.

Condivisione e comunicazione della E-Safety Policy all'intera comunità scolastica

La E-Safety Policy di Istituto si applica a tutti i membri della comunità scolastica: docenti, personale ATA, studenti, genitori e agli utenti che hanno accesso alla scuola.

Il DS regola il comportamento degli studenti e autorizza i docenti a mettere in atto sanzioni per i comportamenti inadeguati, che compromettono la sicurezza online. La scuola si occupa di tali comportamenti e degli incidenti che ne derivano informando i genitori interessati e applicando le sanzioni dovute.

La E-Safety Policy sarà fatta conoscere a tutti i soggetti interessati nei seguenti modi: Pubblicazione della E-Safety Policy sul sito della scuola;

Accordo di utilizzo discusso con i genitori e gli studenti all'inizio del primo anno, tramite il Patto di Corresponsabilità che sarà sottoscritto dalle famiglie e rilasciato alle stesse;

Gestione delle infrazioni alla Policy
La scuola prenderà le precauzioni necessarie per garantire la sicurezza on-line. Malgrado ciò, non è possibile garantire che materiale non adatto comparirà sui computer dell'Istituto o su altri dispositivi mobili. Pertanto la scuola non può accettare la responsabilità per il materiale accessibile e/o le conseguenze di accesso a Internet.
Il Dirigente Scolastico ha la facoltà di revocare l'accessibilità temporanea o permanente ai laboratori informatici e/o all'utilizzo di strumenti tecnologici (pc, tablet, notebook, ecc) a chi non si attiene alle regole stabilite.
Al personale e agli alunni saranno fornite informazioni sulle infrazioni e le relative sanzioni. Le sanzioni includono:

- Informare il coordinatore di classe e il Dirigente Scolastico;
- Informare i genitori,
- Il ritiro del dispositivo usato impropriamente fino a fine giornata;
- Risarcimento (nei modi e nei tempi ritenuti adeguati)
- Sanzioni disciplinari (si veda regolamento disciplinare)
- Eventuale comunicazione alle autorità competenti.

Monitoraggio dell'implementazione della E-Safety Policy e suo aggiornamento
La E-Safety Policy viene approvata dal Collegio dei Docenti e dal Consiglio di Istituto e pubblicate sul sito della scuola. Si inserisce all'interno delle politiche scolastiche relative alla protezione dei minori, contrasto al cyberbullismo e benessere degli alunni a scuola.
La E-Safety Policy sarà revisionata ogni qual volta si verificheranno cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola. Tali modifiche saranno discusse dal Collegio Docenti e condivise con tutto il personale scolastico che è coinvolto nello sviluppo delle linee guida e nell'applicazione delle regole per l'uso sicuro e responsabile delle apparecchiature elettroniche e di Internet.

Formazione

Competenze digitali per gli studenti
L'Istituto si propone di integrare nella progettazione didattica attività che puntano all'acquisizione di competenze e comportamenti che tutelino la sicurezza online degli studenti:

- Migliorare le competenze digitali attraverso il loro uso consapevole;
- Sviluppare strategie per valutare e verificare le informazioni;
- Capire quale sia il comportamento accettabile da mantenere in ambiente online, ossia, essere educato emantenere private le informazioni personali;
- Capire che le immagini possono essere manipolate;
- Capire che quelli che si considerano "amici" online potrebbero non essere chi dichiarano di essere;
- Capire perché non dovrebbero fornire resoconti dettagliati delle loro vite;
- Capire perché non dovrebbero pubblicare o condividere foto e video di altri senza il loro permesso;
- Sapere che scaricare film, video musicali e altri file senza autorizzazione è contro la legge;
- Sapere come segnalare abusi e come chiedere aiuto in caso di pericolo per se stessi o per altri (cyberbullismo, sexting, grooming, ecc).

Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
La Scuola ha previsto:

- Individuazione, fra i docenti, di un Animatore Digitale per l''attuazione degli obiettivi e delle innovazioni previste;
- Individuazione, fra i docenti, di un Referente Bullismo e Cyberbullismo per l'attuazione degli obiettivi e delle innovazioni previste
- Individuazione, di un Amministratore di Sistema per l'attuazione degli obiettivi e delle innovazioni previste
- Eventuale formazione dei docenti all'utilizzo del registro elettronico;
- Organizzazione di corsi per ampliare la conoscenza e l'uso di strumenti digitali da utilizzare nella didattica;
- Formazione del personale in materia di sicurezza online;
- Si assicura che il personale sappia come inviare e ricevere dati sensibili o personali;
- Garantisce le informazioni relative alla E-Safety Policy a tutto il nuovo personale.

Sensibilizzazione delle famiglie
La nostra scuola esegue azioni volte a orientare e informare i genitori tra cui: presentare ai genitori, che iscrivono i propri figli nel nostro Istituto, il Regolamento della E-Safety Policy, così da garantire che i principi di comportamento siano chiari e condivisi.

Gestione dell'infrastruttura e della strumentazione ICT della scuola

Sito web della scuola
L'Istituto possiede un proprio sito web istituzionale all'interno del quale offre una serie di servizi alle famiglie e ai fruitori esterni.
La gestione del sito della scuola è a cura del DS e del Referente sito web istituzionale. La scuola, in qualità di ente pubblico, pubblicherà sul proprio sito contenuti di cui è accertata la rispondenza alle normative per ciò che concerne accuratezza, appropriatezza e aggiornamento.
Le informazioni pubblicate sul sito relative a contatti di personale della scuola o utenti rispetteranno le norme vigenti sulla privacy.
I docenti che desiderano pubblicare materiale riguardante le attività didattiche dovranno chiedere l'autorizzazione al Dirigente.

Social network
L'utilizzo inappropriato dei Social Network con la pubblicazione di nomi o giudizi su persone e istituzioni, come anche, la diffusione di foto/filmati senza il consenso o all'insaputa delle persone coinvolte a norma legge può determinare ricadute di carattere anche penale come ad esempio la diffamazione
Si invitano pertanto tutti gli alunni a non realizzare o diffondere immagini, registrazioni video e audio non autorizzate e ad eliminare da internet qualunque riferimento offensivo o illecito nei confronti dell'Istituto, dei suoi docenti, studenti e delle loro famiglie.
Inoltre si raccomanda agli allievi e ai genitori di fare un uso prudente dei Social Network (in particolare quelli di messaggistica) limitando il loro uso alle sole comunicazioni funzionali all'attività scolastica, senza esprimere giudizi sull'operato degli altri studenti o del personale della scuola poiché tali giudizi, una volta pubblicati, comportano sempre una assunzione di responsabilità da parte di chi li ha scritti o anche solo diffusi.
Il personale dell'Istituto è istruito a mantenere sempre la comunicazione professionale separata da quella personale/privata.
Gli insegnanti, esperti ed educatori sono invitati a non organizzare a titolo personale spazi su Social Network da usare con gli studenti.

Sicurezza rete Lan
L'Istituto dispone di un dominio su rete locale (rete segreteria) cui accedono i computer dell'amministrazione, queste postazioni sono su una rete isolata dal resto della rete dell'Istituto.
La rete interna è protetta da firewall.

Sicurezza della rete Wireless
L'istituto dispone di una rete wi-fi.
La nostra rete wireless assicura standard di sicurezza adatti per l'uso didattico.
Il collegamento di dispositivi personali (PC portatili, tablet, smartphone) alla rete della scuola deve essere autorizzato dai docenti in caso di attività didattiche.
Per garantire che la rete venga utilizzata in modo sicuro, questa scuola chiarisce che:

- E' necessario che tutti gli utenti si disconnettano quando hanno terminato il lavoro o sono obbligati a lasciare il computer incustodito.
- E' vietato di utilizzare sessioni lasciate per errore aperte da utenti precedenti. In tali casi è obbligatorio uscire dalla sessione mediante logout ed informare l'utente.
- Assicura a tutte le apparecchiature di proprietà della scuola una adeguata protezione antivirus e firewall
- Utilizza il trasferimento e mantenimento sicuro dei dati (pec o in modalità crittografata).
- Assicura che tutti i dati sensibili degli allievi o del personale inviati via Internet vengano crittografati o inviati e archiviati con sistema sicuro.
- Tutte le TIC e i sistemi di comunicazione sono stati installati da professionisti del settore e sono regolarmente verificati per assicurare che soddisfino gli standard di salute e sicurezza.

Protezione dei dati personali
L'Istituto rispetta la privacy dei propri utenti e si impegna a proteggere i dati personali degli stessi.
L'utente può navigare sul sito web dell'Istituto senza fornire alcun tipo di informazione personale.
La raccolta ed il trattamento di dati personali avvengono, quando necessari, in relazione all'esecuzione di servizi richiesti dall'utente, o quando l'utente stesso decide di comunicare i propri dati personali; in tal caso i dati personali verranno trattati in conformità alla normativa vigente.
In caso di raccolta di dati personali, l'Istituto informerà l'utente sulle finalità della raccolta al momento della stessa, ove necessario, richiederà il consenso dell'utente.

Strumentazione personale

Gestione degli strumenti personali (PC, tablet)
Come riportato nel regolamento d'Istituto agli studenti non è permesso utilizzare i propri smartphone all'interno della scuola. PC e tablet possono essere utilizzati alla presenza del docente e solo per scopi didattici, senza connessione web, salvo diverse indicazioni da parte del docente.

Prevenzione, rilevazione e gestione dei casi

Pagina web istituzionale: https://web.liceogiovio.edu.it/_sito2020/index.php/didattica/progetti-ministeriali/bullismo-e-cyberbullismo

Prevenzione
La Scuola ha scelto una politica interna che punta a creare un ambiente di apprendimento sereno e sicuro in cui sia chiaro che prepotenza, aggressione, violenza, bullismo e cyberbullismo non sono tollerati, che stimoli la partecipazione di tutta la comunità scolastica nelle azioni finalizzate al contrasto di tali comportamenti, che insegni ad interagire in maniera responsabile e che incoraggi l'apertura necessaria a parlare di sé e dei propri problemi.
Per attuare questo tipo di politica è necessaria la creazione di una comunità solidale, in cui ogni allievo ha il diritto di vivere una scuola senza violenza e allo stesso tempo ha il dovere di difendere i compagni più vulnerabili. Il coinvolgimento degli alunni è indispensabile per creare un clima di solidarietà, combattere l'omertà e l'indifferenza, incoraggiare le vittime a chiedere aiuto.
Per quanto riguarda le attività online i principi generali sono:

- Quando si utilizzano Social Network e Applicazioni bisogna informarsi su quali siano diritti e doveri dell'utente leggendo i regolamenti e tenendosi aggiornati visitando siti istituzionali tematici;
- E' sempre meglio non condividere informazioni personali, ma se ciò fosse necessario bisogna farlo scegliendo con cura cosa rendere pubblico e cosa mantenere privato. Bisogna proteggere la propria Identità Digitale utilizzando password complesse (alfanumeriche, con caratteri maiuscoli e minuscoli e simboli grafici);
- Se si condividono contenuti multimediali e informazioni che coinvolgono più persone è necessario avere l'autorizzazione di ogni utente prima di effettuare la pubblicazione;
- Quando un utente commette involontariamente un abuso o un errore, pubblicando materiale non idoneo, offensivo o illecito, bisogna contattarlo e informarlo delle regole relative alla sicurezza.
- Qualunque abuso rilevato o subito online, deve essere segnalato mediante gli strumenti offerti dal servizio. Tutti i socia network garantiscono la possibilità di segnalare attività inopportune e la rimozione dei contenuti non adeguati. Qualora la segnalazione rimanesse inevasa ci si può rivolgere al Garante della Privacy.

Rischi
La forma di bullismo online o cyberbullismo ha alcune caratteristiche che la rendono particolarmente pericoloso:

- Il cyberbullismo è pervasivo perché il cyberbullo può raggiungere la vittima in qualsiasi luogo e in qualsiasi momento;
- E' un fenomeno persistente poiché i file offensivi o diffamatorio, una volta condivisi, rimangono online e non è più possibile controllarli o eliminarli definitivamente;
- Spettatori e cyberbulli sono potenzialmente infiniti;
- Esattamente come accade per il bullismo, tutti quelli che osservano senza far nulla diventano corresponsabili delle azioni del cyberbullo. E' quindi chiaro che chiunque detenga, condivida o commenti foto o video si fa carico di una responsabilità diretta.

Azioni
Le azioni messe in atto dall'Istituto sono volte a sensibilizzare gli alunni verso un uso responsabile e consapevole della rete, con la finalità di tutelarli da abusi e violenze da un lato e, allo stesso tempo, suscitare atteggiamenti di rispetto nei confronti degli altri utenti.
La nostra Scuola si impegna:

- Interventi formativi.
- Elaborare un proposta di approccio curricolare inserendo attività di sensibilizzazione nell'azione didattica da svolgere in classe a cura dei docenti, utilizzando filmati, episodi di cronaca recenti o testi come stimolo per la discussione in classe, l'acquisizione di consapevolezza del problema, delle motivazioni sottostanti e delle conseguenze e la promozione di un sistema di regole e di una cultura contro le prepotenze nella classe; Implementare la e-Safety Policy con il contributo di tutte le componenti (docenti, studenti, famiglie, personale A.T.A.);
- Presentare la e-Safety Policy così redatta agli Organi Collegiali e quindi inserirla nel sistema di regolamenti della Scuola e renderla pubblica sul sito della Scuola garantendone la massima diffusione e condivisione.

Rilevazione
La nostra scuola è impegnata nel coinvolgimento della comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online. I casi rilevati verranno gestiti mettendo in atto azioni diverse. Da un lato si informeranno gli alunni e i genitori selle consegue relative al fenomeno emerso, dall'altro si cercherà di aiutare gli alunni coinvolti creando situazioni dialogo che consentano di far emergere gli aspetti di criticità sui quali, mediante riflessione, si potrà intervenire.

Sportello Bullismo-Cyberbullismo
Che cos'è?
E' uno spazio di ascolto di problematiche e disagi legati a episodi di bullismo e finalizzato al miglioramento della convivenza serena tra gli alunni e alla promozione del benessere a scuola. Per gli studenti è un momento di condivisione di dubbi, paure, disagi, raccolta di informazioni e consigli. Per i genitori è un momento di confronto, conforto, messa a punto di strategie per aiutare i propri ragazzi. Per la scuola nel suo insieme è un modo di stringersi attorno ai propri studenti che stanno attraversando un momento di difficoltà e far loro capire che la scuola è pronta a mettere in atto misure adeguate.

Cosa non è?
Non è un percorso di psicoterapia. Le informazioni condivise in questo spazio sono riservate e condivise con terzi solo in casi ritenuti necessari dalla Dirigenza e/o previsti dalla normativa vigente.

A chi si rivolge?
A docenti, studenti e famiglie che desiderano segnalare problematiche legate ai fenomeni di bullismo e cyberbullismo in uno spazio protetto e soggetto alla assoluta riservatezza delle informazioni raccolte, se non nei casi in cui si renda necessaria una condivisione con Dirigente, figure specifiche, esperti esterni.

Studenti: possono recarsi autonomamente all'incontro con la referente avvisando il docente in orario. Lo studente che si reca allo sportello è da ritenersi giustificato presso il docente. Si confida nella collaborazione di tutti i docenti per favorire l'accesso allo sportello in quanto il benessere a scuola è da ritenersi di primaria importanza. Per gli studenti minori è necessaria **autorizzazione** dei genitori.

Genitori: possono richiedere un appuntamento online via email all'indirizzo **sosbullismo@liceogiovio.edu.it** e verrà inviato il link di accesso alla riunione.

Protocollo per le emergenze
La scuola nomina un Team specializzato per la gestione delle emergenze, il quale deve essere individuato tra figure in ambiente scolastico ma anche extra-scolastico, le quali devono avere competenze, responsabilità, tempi e modalità di azione specifici. Il team è composto dai seguenti membri:

- DIRIGENTE SCOLASTICO
- REFERENTE BULLISMO E CYBERBULLISMO
- UN GENITORE DEL CONSIGLIO DI ISTITUTO
- UNO STUDENTE DEL CONSIGLIO DI ISTITUTO
- PSICOLOGI DI ISTITUTO

Il team di gestione delle emergenze redige un piano di azione che si articola in quattro fasi:

1. Prima segnalazione ha lo scopo di accogliere la segnalazione di tutti i presunti casi di bullismo in modo da poter prendere in carico la situazione. Il caso potrà essere riferito da qualsiasi persona interna o esterna della scuola. La prima segnalazione ha lo scopo di attivare un processo di attenzione e di successiva valutazione rispetto ad un presunto caso di bullismo o cyberbullismo: serve quindi a fare in modo che tutte le potenziali situazioni di sofferenza non vengano sottovalutate e ritenute erroneamente poco importanti.

2. Valutazione del caso:
Il passo successivo alla prima segnalazione è quello di svolgere una valutazione più approfondita dell'accaduto attraverso colloqui con le persone coinvolte.
Lo scopo è quello di valutare la tipologia e la gravità per poter definire il successivo tipo di intervento. La valutazione approfondita viene condotta dal Referente antibullismo, eventualmente coadiuvato dal Team per l'Emergenza. La valutazione potrebbe essere fatta potenzialmente con tutti gli autori direttamente e indirettamente coinvolti: chi ha fatto la prima segnalazione, vittima, compagni testimoni, insegnanti di classe, genitori, bullo/i. La scelta della modalità dipende dal tipo di situazione. Le aree di approfondimento riguardano: l'evento, le persone coinvolte nei diversi ruoli, la tipologia di comportamento e la loro durata.

3. Scelta dell'intervento:
Sulla base delle informazioni acquisite nelle diverse sezioni (gravità della sintomatologia della vittima, gravità della sintomatologia del bullo, caratteristiche del quadro contestuale del gruppo-classe e della famiglia), si delinea il livello di priorità dell'intervento, che va da un livello meno grave (verde), a un livello sistematico più grave (giallo) fino ad un livello molto grave di emergenza (rosso). In base al livello verranno poi delineate le azioni da intraprendere. Il team per l'emergenza una volta decisa la tipologia di intervento da attuare, ha il compito di coinvolgere le altre figure che supporteranno nella realizzazione dell'intervento/ degli interventi (es. i docenti della classe per l'intervento educativo con la classe)
Caso di codice verde:
La situazione deve essere affrontata, e monitorata, con interventi da attuare in classe tramite un approccio educativo. Si può inoltre pensare di coinvolgere alcuni studenti in particolare (es. difensore della vittima) per alcuni interventi mirati (es. supporto).
Caso di codice giallo:
Nel caso di un codice giallo (livello sistematico di bullismo e di vittimizzazione), la situazione deve essere affrontata con interventi da attuare in classe, con interventi individuali svolti con il bullo e/o la vittima e tramite il coinvolgimento della famiglia. Ad esempio, un primo obiettivo potrebbe essere quello di sensibilizzare la classe verso il fenomeno del bullismo e cyberbullismo al fine di aumentare la consapevolezza relativa al fenomeno, alle emozioni e alle conseguenze per la vittima e l'importanza del ruolo degli spettatori passivi). Potrebbe essere svolto, inoltre, un intervento individuale che coinvolga il bullo e/o la vittima che potrebbe essere effettuato dallo psicologo della scuola e/o da professionisti esterni. Infine potrebbe essere utile informare e coinvolgere anche la famiglia
Caso di codice rosso:
Nel caso di un codice rosso (livello di urgenza di bullismo e di vittimizzazione), dovranno essere utilizzati interventi di emergenza quali:

- Approccio educativo con l'intera classe svolto dall'insegnate;
- Coinvolgimento tempestivo della famiglia da parte del Dirigente Scolastico e dal team per l'emergenza;
- Supporto intensivo per la vittima;
- Intervento dello psicologo sui bulli;
- Supporto intensivo a lungo termine e di rete (Accesso ai servizi del territorio, per esempio consultori di riferimento, attraverso il dirigente scolastico, team e famiglia).

4. Monitoraggio nel tempo:
Dopo la segnalazione del caso, la valutazione approfondita e la scelta dell'intervento/degli interventi, una volta messe in atto la/le diverse azioni, il passaggio successivo sarà quello del monitoraggio. Lo scopo generale è quello di valutare l'eventuale cambiamento a seguito dell'intervento/degli interventi (es. sono terminati i comportamenti di bullismo messi in atto verso la vittima) e se tale miglioramento della situazione rimanga stabile nel tempo (es. non si ripresentino prese in giro dopo qualche settimana quando l'attenzione sul caso potrà sembrare diminuita). In particolare, si dovrebbero prevede almeno due momenti: a breve termine, entro una settimana; a lungo termine dopo circa un mese.

Altre azioni del Team di emergenza:
Il Team di emergenza, oltre all'analisi della gravità dei fatti accaduti, valuta il livello di rischio e di sofferenza psicologica delle singole persone coinvolte. Potrebbe essere opportuno richiedere un supporto esterno alla scuola nei casi in cui gli atti di bullismo e cyberbullismo subiti e agiti siano molto gravi, la sofferenza della vittima sia elevata o la compromissione nel funzionamento sociale, il livello dei comportamenti aggressivi e a rischio dei bulli siano considerevoli.

Il Dirigente Scolastico e il Team in collaborazione, con la famiglia, possono gestire la situazione richiedendo un supporto intensivo a lungo termine e di rete in collaborazione, a seconda del caso, con i Servizi Sanitari Territoriali, i Servizi sociali, gli ospedali, il Pronto soccorso, la Polizia Postale, i Carabinieri o altri enti e associazioni presenti sul territorio.

Supporto sul territorio:

C'è una grande variabilità rispetto ai canali di comunicazione e collaborazione tra le scuole e il territorio.

Per una ricognizione a livello regionale, è stato realizzato un *Vademecum* nell'ambito del progetto GenerazioniConnesse SIC III – Safer Internet Centre Italia, co-finanziato dalla Commissione Europea e coordinato dal Ministero dell'Istruzione, dell'Università e della Ricerca, in partenariato con l'Autorità Garante per l'Infanzia e l'Adolescenza, la Polizia di Stato, Save the Children Italia, SOS - Il Telefono Azzurro Onlus, la Cooperativa E.D.I., il Movimento Difesa del Cittadino e Skuola.net, Agenzia Dire Giovani.

Il vademecum nasce come una guida operativa con l'obiettivo di diffondere, soprattutto a livello territoriale, strumenti conoscitivi ed operativi utili per orientarsi nella gestione di alcune problematiche inerenti l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC) da parte dei più giovani. La lista di servizi e istituzioni di cui sono forniti indirizzi e riferimenti telefonici, segue una suddivisione regionale, e può essere un'utile risorsa per reperire risorse e supporto nei casi di bullismo e cyberbullismo.

Si rivolge, in particolare, a genitori, insegnanti, operatori del sociale e della salute mentale, a professionisti dell'infanzia e, in generale, a tutti coloro che sono coinvolti nelle tematiche in questione o semplicemente interagiscono con il mondo giovanile e intendono acquisire maggiore strumenti conoscitivi e operativi sui rischi collegati all'utilizzo delle TIC.

Il documento, sicuramente non esaustivo, rappresenta un primo tentativo di raccolta e sistematizzazione di informazioni non sempre note o facilmente accessibili e quindi, speriamo, utili ad un primo orientamento qualora ci si trovi a dover affrontare una delle tematiche trattate.

Il documento è strutturato in due parti:

- Una prima sezione dedicata all'approfondimento di alcune problematiche legate all'uso delle TIC (es. il cyberbullismo, la pedopornografia online, l'adescamento online, etc.);
- **Una sezione con i riferimenti dei servizi a cui è possibile rivolgersi a livello regionale.**

Qui si può scaricare il vademecum completo.

Allegati (si vedano pagine seguenti)

Delibera del Collegio dei Docenti del 23.03.2026

Delibera del Consiglio di Istituto del 25.05.2026

MINISTERO DELL'ISTRUZIONE E DEL MERITO

Liceo Scientifico Linguistico Statale "Paolo Giovio"

ALLEGATO N. 1

PRIMA SEGNALAZIONE

Inviare e-mail alla Referente Bullismo e Cyberbullismo

alessandra.cuomo@liceogiovio.edu.it

Nella stesura dell'email devono essere presenti i punti segnalati nella presente scheda

Nome di chi compila la segnalazione:

Data:

1. La persona che ha segnalato il caso è
   - ❑ La vittima
   - ❑ Un compagno della vittima, nome_____
   - ❑ Madre/ Padre/Tutore della vittima, nome_____
   - ❑ Insegnante, nome _____
   - ❑ Altri: _____

2. Vittima _____Classe_____
   Altre vittime _____Classe_____
   Altre vittime _____Classe_____

3. Bullo o i bulli (o presunti)
   Nome_____Classe_____
   Nome_____Classe_____
   Nome_____Classe_____

4. Descrizione breve del problema presentato. Dare esempi concreti degli episodi di prepotenza.
5. Quante volte sono successi gli episodi?

MINISTERO DELL'ISTRUZIONE E DEL MERITO

Liceo Scientifico Linguistico Statale "Paolo Giovio"

ALLEGATO N. 2

SCHEDA DI VALUTAZIONE APPROFONDITA DEI CASI DI BULLISMO/CYBERBULLISMO E VITTIMIZZAZIONE

Nome del membro del team che compila lo screening: _____
Data: _____
Plesso: _____
Data della segnalazione del caso di bullismo: _____
1. La persona che ha segnalato il caso di bullismo era:
o La vittima
o Un compagno della vittima, nome
o Madre/ Padre della vittima, nome
o Insegnante, nome
o Altri:
2. Nome e ruolo della persona della scuola che ha compilato il modulo del pre-screening:
_____
3. Vittima, nome _____ classe: _____
Altre vittime, nome _____ classe: _____
Altre vittime, nome _____ classe: _____
4. Il bullo o i bulli
Nome _____ classe: _____
Nome _____ classe: _____
Nome _____ classe: _____
5. Che tipo di prepotenze sono accadute? Dare esempi concreti degli episodi.
_____
_____
_____

6. In base alle informazioni raccolte, che tipo di bullismo è avvenuto?
a) è stato offeso, ridicolizzato e preso in giro in modo offensivo;
b) è stato ignorato completamente o escluso dal suo gruppo di amici;
c) è stato picchiato, ha ricevuto dei calci, o è stato spintonato;
d) sono stati messe in giro bugie/voci che hanno portato gli altri a "odiarlo";
e) gli sono stati presi dei soldi o altri effetti personali (o sono stati rotti);
f) è stato minacciato o obbligato a fare certe cose che non voleva fare;
g) gli hanno dato dei brutti nomi, hanno fatto brutti commenti o gesti sulla sua etnia, colore della pelle, religione, orientamento sessuale o identità di genere;
h) ha subito delle offese o molestie sessuali, attraverso brutti nomi, gesti o altro;
i) è stato escluso da chat di gruppo, da gruppi WhatsApp, o da gruppi online;
l) ha subito le prepotenze online tramite computer o smartphone con messaggi offensivi, post o fotografie su Facebook, su WhatsApp, Twitter, Myspace, Snapchat o tramite altri social media;
m) ha subito appropriazione di informazioni personali e utilizzo sotto falsa identità della propria password, account (e-mail, Facebook...), rubrica del cellulare...
Altro:
_____
_____

7. Quante volte sono successi gli episodi di bullismo?
_____
8. Quando è successo l'ultimo episodio di bullismo?
_____
9. Da quanto tempo il bullismo va avanti?
_____

10. Si sono verificati episodi anche negli anni precedenti?

_____

11. Analisi della situazione della vittima e del bullo:

Sofferenza della vittima:

La vittima presenta…	Non vero	In parte – Qualche Volta	vero –	Molto spesso vero

o Cambiamenti rispetto a come era prima
o Ferite o dolori fisici non spiegabili
o Paura di andare a scuola (non va volentieri)
o Paura di prendere l'autobus – richiesta di essere accompagnato – richiesta di fare una strada diversa
o Difficoltà relazionali con i compagni
o Isolamento / rifiuto
o Bassa autostima
o Cambiamento nell'umore generale (è più triste, depressa, sola/ritirata)
o Manifestazioni di disagio fisico- comportamentale (mal di testa, mal di pancia, non mangia, non dorme...)
o Cambiamenti notati dalla famiglia
o Impotenza e difficoltà a reagire

Gravità della situazione della vittima:

A. Presenza di tutte le risposte con livello 1 (non vero)= VERDE
B. Presenza di almeno una risposta con livello 2 (In parte, qualche volta) = GIALLO
C. Presenza di almeno una risposta con livello 3 (molto vero, spesso)= ROSSO

Sintomatologia del bullo:

Il bullo presenta…	Non vero	In parte – Qualche Volta	vero –	Molto spesso vero

o Comportamenti di dominanza verso i pari
o Comportamenti che prendono di mira i compagni più deboli
o Uno status per cui gli altri hanno paura di lui/lei
o Mancanza di paura/preoccupazione per le conseguenze delle proprie azioni
o Assenza di sensi di colpa (se e rimproverato non dimostra sensi di colpa)
o Comportamenti che creano pericolo per gli altri
o Cambiamenti notati dalla famiglia

Gravità della situazione del bullo:

A. Presenza di tutte le risposte con livello 1 = VERDE
B. Presenza di almeno una risposta con livello 2 = GIALLO
C. Presenza di almeno una risposta con livello 3 = ROSSO

12. Fenomenologia del bullismo: il gruppo e il contesto

1. Da quanti compagni è sostenuto il bullo? _____
2. Gli studenti che sostengono attivamente il bullo:

Nome _____ classe: _____
Nome _____ classe: _____
Nome _____ classe: _____

3. Quanti compagni supportano la vittima o potrebbero farlo?_____

Gli studenti che possono sostenere la vittima:

Nome _____ classe: _____
Nome _____ classe: _____
Nome _____ classe: _____

4. Gli insegnanti sono intervenuti in qualche modo? _____
5. La famiglia o altri adulti hanno cercato di intervenire? _____
6. La famiglia ha chiesto aiuto? _____

DECISIONE

In base alle informazioni acquisite dalle diverse sezioni (gravità della sintomatologia della vittima, gravità della sintomatologia del bullo, caratteristiche del quadro contestuale del gruppo classe e della famiglia), si delinea come livello di priorità dell'intervento:

LIVELLO DI RISCHIO DI BULLISMO E VITTIMIZZAZIONE: CODICE VERDE
Situazione da monitorare con interventi preventivi nella classe
LIVELLO SISTEMATICO DI BULLISMO E VITTIMIZZAZIONE: CODICE GIALLO
Interventi indicati e strutturati a scuola e in sequenza coinvolgimento della rete se non ci sono risultati
LIVELLO DI URGENZA DI BULLISMO E VITTIMIZZAZIONE: CODICE ROSSO
Interventi di emergenza con supporto della rete

MINISTERO DELL'ISTRUZIONE E DEL MERITO

Liceo Scientifico Linguistico Statale "Paolo Giovio"

ALLEGATO N. 3

SCHEDA DI MONITORAGGIO

PRIMO MONITORAGGIO

In generale la situazione è:

o Migliorata

o Rimasta invariata

o Peggiorata

Descrivere come:

SECONDO MONITORAGGIO

In generale la situazione è:

o Migliorata

o Rimasta invariata

o Peggiorata

Descrivere come:

TERZO MONITORAGGIO

In generale la situazione è:

o Migliorata

o Rimasta invariata

o Peggiorata

Descrivere come:

QUARTO MONITORAGGIO

In generale la situazione è:

o Migliorata

o Rimasta invariata

o Peggiorata

Descrivere come: