



**MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITA' E DELLA RICERCA UFFICIO
SCOLASTICO REGIONALE PER IL LAZIO
ISTITUTO D'ISTRUZIONE SUPERIORE VIA GRAMSCI**

REGOLAMENTO D'ISTITUTO PER LA PREVENZIONE E IL CONTRASTO DEL BULLISMO E CYBERBULLISMO

**Il presente Regolamento è da intendersi come parte integrante del vigente
Regolamento di Istituto**

(Approvato dal Consiglio di Istituto con Delibera n.41 del 07/01/2021)

Titolo 1 - Il documento di E-Policy

Introduzione

La scuola rappresenta il luogo in cui gli studenti quotidianamente sperimentano i processi di apprendimento, vivendo opportunità di crescita intellettuale, di maturazione, di acquisizione di consapevolezza critica e di responsabilità. La presenza sempre più diffusa delle tecnologie digitali nella vita di tutti i giorni, compresi gli ambienti scolastici, apre nuove opportunità, ma pone nuove attenzioni dal punto di vista del loro uso sicuro, consapevole e positivo. Gli adulti hanno un ruolo fondamentale nel garantire che i giovani siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato e sicuro, ruolo che vede coinvolti a pieno titolo tutti coloro che hanno un ruolo educativo, oltre che formativo, in altre parole la comunità scolastica nel suo complesso, genitori inclusi. E' in questo quadro che si inserisce la necessità di affrontare la questione da più punti di vista e interessando più interlocutori, inclusi i più giovani, per arrivare a dotare ogni comunità scolastica di una propria E- Policy.

In particolare il documento risponde alle Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo delineate dalla Legge del 29 maggio 2017, n. 71, entrata in vigore il 18 giugno 2017 e pubblicata in Gazzetta Ufficiale il 3 giugno 2017.

Art. 1 Scopo dell'E-Policy

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 quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E-policy vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti ed 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 (TIC) in ambiente scolastico; le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio; le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali

Art. 2 - Ruoli e responsabilità

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

- Il **Dirigente scolastico** è garante per la sicurezza di tutti i membri della comunità scolastica. Promuove ed attiva buone prassi secondo le indicazioni del M.I.U.R., mediante l'organizzazione di percorsi di formazione per la sicurezza e problematiche connesse all'utilizzo della rete sia online che offline, con la collaborazione del docente Referente d'Istituto per le tematiche del Bullismo e del Cyberbullismo, fermo restando la responsabilità di gestire ed intervenire nei casi di gravi episodi ed uso improprio delle tecnologie digitali degli studenti e delle studentesse.
- Il **Referente d'Istituto per la prevenzione ed il contrasto del Bullismo e del Cyberbullismo**, individuato ai sensi dell'art. 4, comma 3, Legge 29 maggio 2017, n. 71, ha il compito di "coordinare le iniziative di prevenzione e di contrasto del cyberbullismo, anche avvalendosi della collaborazione delle Forze di polizia nonché delle associazioni e dei centri di aggregazione giovanile presenti sul territorio". Il suo ruolo è importante non solo in ambito scolastico ma anche in quello extrascolastico (ove possibile), per il coinvolgimento in percorsi formativi finalizzati per studenti e studentesse, per genitori e per l'intera comunità scolastica.
- L'**Animatore digitale** rappresenta un valido supporto per l'intero personale scolastico non solo dal punto di vista tecnico-informatico, ma anche in riferimento alla protezione e gestione dei dati personali, rischi online, e per buone prassi in materia di percorsi di formazione "scuola digitale" ed "educazione civica".
- I **Docenti** hanno un ruolo centrale nel "diffondere la cultura dell'uso responsabile delle TIC e della Rete", accostando alla didattica l'utilizzo delle tecnologie digitali, ove possibile. Supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici, che si connettono alla Rete; hanno il "dovere morale e professionale di segnalare al Dirigente scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse".

- Il **Personale Amministrativo, Tecnico ed Ausiliario** (ATA), svolge funzioni di tipo amministrativo, contabile, gestionale e di sorveglianza, connesse alle attività dell'Istituzione scolastica, in collaborazione con il Dirigente scolastico e con il personale docente tutto. È coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo insieme alle figure interne preposte, e nel raccogliere, verificare e valutare le informazioni inerenti a possibili casi di bullismo e di cyberbullismo.
- Gli **Studenti e le Studentesse** sono tenuti/e al rispetto delle norme che disciplinano l'utilizzo consapevole delle tecnologie digitali con la finalità di salvaguardare la propria identità e quella altrui, secondo quanto indicato nel Regolamento d'Istituto. La partecipazione a percorsi formativi e progettuali ha lo scopo di promuovere l'utilizzo positivo delle TIC e della Rete, in una dimensione di peer education. I genitori sono corresponsabili nelle scelte educative dell'Istituzione scolastica, atte alle attività di prevenzione ed uso consapevole delle TIC, della Rete e dei device personali dei rispettivi figli.
- Gli **Enti educativi esterni e le Associazioni** che entrano in relazione con l'Istituzione scolastica, osservano le politiche interne sull'uso consapevole della Rete e delle TIC, fermo restando di attivare procedure e comportamenti sicuri per la protezione degli studenti e delle studentesse, durante le attività che vengono svolte all'interno della scuola o in cui sono impegnati gli stessi.

Per quanto non espressamente indicato sui ruoli e sulle responsabilità delle figure presenti all'interno dell'Istituzione scolastica, si rimanda: all'art. 21, comma 8, Legge 15 marzo 1997, n. 59; all'art. 25 della Legge 30 marzo 2001, n. 165; al CCNL in vigore; al D.P.R. 8 marzo 1999, n. 275; alla Legge 13 luglio 2015, n. 107; al Piano Nazionale Scuola Digitale; a quanto statuito in materia di culpa in vigilando, culpa in organizzando, culpa in educando.

Art. 3 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 ed 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, etc.) e 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, mail, chat, profili di social network).

Art. 4 Condivisione e comunicazione dell'E-Policy

Il documento di E-policy 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/le studenti/esse) si faccia a sua volta promotore del documento.

L'E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico.

Il documento è approvato dal Consiglio di Istituto. Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

Art. 5 Gestione delle infrazioni alla E-Policy

Sulla base dello Statuto delle studentesse e degli studenti e del Regolamento d'Istituto gli studenti protagonisti di atti di bullismo sono coinvolti in un percorso di comprensione della gravità degli atti compiuti e, se possibile, a mettere in atto comportamenti attivi riparatori (es. attività di volontariato, pulizia degli spazi scolastici, piccole manutenzioni, svolgimento di attività di assistenza o di volontariato nell'ambito della comunità scolastica o delle associazioni del territorio convenzionate.)

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

Infrazione/sanzione degli alunni

Viene individuato come organo competente per la gestione delle infrazioni dei singoli alunni il Consiglio di Classe. I provvedimenti disciplinari da adottare nei confronti dell'alunno che ha commesso un'infrazione alla Policy, dopo aver tenuto conto sia dell'età dell'alunno che della gravità dell'infrazione commessa, saranno i seguenti:

- **richiamo verbale:** il singolo docente che riscontra la mancanza o il Dirigente Scolastico provvede al richiamo verbale e ne dà notizia nel registro di classe;
- **ammonizione scritta:** il singolo docente che riscontra la mancanza o il Dirigente Scolastico provvede all'annotazione dell'ammonizione nel registro di classe valutando l'opportunità di comunicare l'ammonizione ai genitori. Il Dirigente Scolastico può valutare l'opportunità di convocare i genitori dell'alunno sanzionato;
- **studio di un argomento scelto dal Dirigente Scolastico,** con valutazione finale, quando l'alunno abbia dato prova di scarsa maturità o di disinteresse per le regole scuola ed in genere per le regole della convivenza civile, può essere invitato dal Dirigente Scolastico ad approfondire alcune tematiche (ad es. il concetto di responsabilità, il concetto di sanzione, la condizione del minore, il bullismo) con successiva valutazione in occasione di una esposizione orale che si svolgerà secondo le modalità definite dal Dirigente scolastico stesso. Tale valutazione non influisce sul profitto ma è un elemento di cui il Consiglio di Classe può tenere conto ai fini dell'attribuzione del voto di condotta;
- **esclusione/sospensione dell'alunno dalla partecipazione ad attività non curricolari:** il singolo docente o il coordinatore di classe che abbiano riscontrato una mancanza grave o una reiterazione di una mancanza lieve provvedono ad informare il Dirigente scolastico fornendo adeguate indicazioni sui fatti accaduti. Il Dirigente Scolastico, considerato il comportamento dell'alunno, valuta l'opportunità di comminare tale sanzione o, in alternativa, di convocare il Consiglio di Classe per la comminazione delle sanzioni più gravi. L'esclusione/sospensione dell'alunno dalla partecipazione ad attività non curricolari è disposta quando la mancanza grave o la reiterazione della mancanza lieve faccia ritenere inopportuna la partecipazione dell'alunno all'attività non curricolare;
- **temporaneo allontanamento dell'alunno dalla Comunità scolastica per periodi non superiori a 15 giorni:** il Dirigente Scolastico informato dal singolo docente o dal coordinatore di classe del fatto che può comportare tale tipo di sanzione, avvia la procedura mediante convocazione del Consiglio di classe (entro 8 giorni dalla notizia del fatto), ivi compresi gli studenti e i genitori (salvo il dovere di astensione dello studente e/o del genitore dello studente da sanzionare, nel qual caso si procederà ad una surroga) e comunica l'avvio del procedimento all'alunno e alla famiglia. Il Consiglio di classe, verificata la sussistenza di elementi concreti e precisi dai quali si desume che l'infrazione

disciplinare è stata effettivamente commessa da parte dell'alunno incolpato, decide la misura della sanzione. Il provvedimento viene annotato nel registro di classe e notificato alla famiglia con le modalità già previste dal regolamento di istituto ivi ricompreso eventuale ricorso all'organo di garanzia. Durante il periodo di allontanamento la scuola assicura un rapporto con lo studente e con i suoi genitori per preparare il rientro dell'alunno nella comunità scolastica;

●-**temporaneo allontanamento dell'alunno dalla Comunità scolastica per periodi superiori a 15 giorni;**

- **allontanamento dello studente dalla comunità scolastica fino al termine dell'anno scolastico;**

- **esclusione dallo scrutinio finale o non ammissione all'esame di Stato conclusivo del corso di studi.**

Nei casi sopra indicati, il consiglio di classe, valutata la gravità dell'infrazione disciplinare, qualora ritenga opportuno che la sanzione da comminare valichi le proprie competenze, previa verifica della sussistenza di elementi dai quali si possa evincere la responsabilità disciplinare dello studente, comunica al dirigente, con apposita delibera, la necessità di avviare il procedimento innanzi al Consiglio d'Istituto. Il Dirigente scolastico, si adopererà, nei tempi e nelle forme di cui alla lettera precedente, per la convocazione del consiglio di istituto.

Art. 6 Monitoraggio dell'implementazione della Policy e suo aggiornamento

Nel mese di maggio di ogni anno scolastico il Dirigente Scolastico, il Referente per il Bullismo e Cyberbullismo e l'Animatore digitale si riuniranno con l'obiettivo di esaminare situazioni problematiche riscontrate durante l'anno e la loro gestione, in tale occasione valuterà la necessità o meno di modificare o implementare la Policy.

Art. 7 Integrazione della Policy con regolamenti esistenti

Il presente documento si integra pienamente per obiettivi e contenuti con il PTOF, incluso il piano per l'attuazione del PNSD e con i regolamenti già in vigore nell'Istituto quali:

- Regolamento interno d'istituto;
- Regolamento per l'utilizzo dei laboratori.

Titolo 2 - Formazione e curriculum

Art. 1 Curricolo sulle competenze digitali per gli studenti

Per il curricolo sulle competenze digitali si fa riferimento alle competenze disciplinari individuate dei singoli Dipartimenti.

Art. 2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica e sull'uso consapevole di Internet e delle tecnologia digitali

Le attività di formazione si svolgeranno su due livelli:

- Formazione istituzionale, organizzata dal Miur secondo il PNSD, attraverso gli snodi formativi;
- Formazione specifica di Istituto, legata alle esigenze formative rilevate ad inizio d'anno dal Collegio Docenti.

All'inizio di ogni anno scolastico il Referente per il Bullismo e Cyberbullismo, valutato a quali progetti/iniziative aderire e quali attività svolgere durante l'anno in corso, presenterà le sue proposte al Collegio Docenti per l'approvazione e la condivisione.

Art. 3 Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Nella prevenzione dei rischi connessi ad 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 verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di 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.

Sarà creato sul sito della scuola un'area dedicata alla sicurezza in rete nella quale saranno inseriti materiali che illustrano i principali rischi che può incontrare un adolescente attraverso la navigazione in rete. Tali materiali affronteranno tematiche quali il cyberbullismo, il sexting e l'adescamento. La scuola darà inoltre ampia diffusione, tramite pubblicazione sul sito, del presente documento di Policy per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e per favorire un'attiva collaborazione

tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi a un uso inappropriato del digitale.

Titolo 3 - Gestione dell'infrastruttura e della strumentazione ICT della e nella scuola

Art. 1. Accesso ad Internet, Gestione accessi (password) e Accesso alla strumentazione di istituto (LIM – PC – Laboratori)

L'accesso ad internet è possibile in tutti i plessi dell'Istituto, consentito al solo personale scolastico e solo relativamente alle attività laboratoriali.

Il controllo degli accessi, il monitoraggio ed il filtraggio dei contenuti nonché la conservazione dei log delle suddette attività viene gestita da un Firewall di protezione. Gli accessi di amministrazione sono in possesso della dirigenza scolastica, del Preposto all'amministrazione di rete nominato dalla dirigenza scolastica e della ditta Edit Informatica.

L'accesso alla rete dell'istituto avviene tramite autentica basata su voucher. Ciascun docente è in possesso del proprio codice personale, necessario per l'accesso alla rete.

L'accesso a tutti i PC, i tablet e le LIM dell'istituzione scolastica avviene tramite doppio account:

- uno riservato al personale responsabile della manutenzione e dell'aggiornamento (assistenti tecnici) che ne possiede, oltre alla dirigenza, username e password
- uno accessibile al personale docente (con password comune diffusa tramite l'area riservata del sito) o agli alunni (PC di laboratorio) sotto sorveglianza dei docenti o degli assistenti di laboratorio (con password diversa per ciascuna classe).

A questi ultimi account non è consentito scaricare contenuti.

SICUREZZA

Al fine di garantire il rispetto dei dati sensibili, la protezione da attacchi di natura informatica ed al contempo impedire la fruizione di contenuti non ammissibili in ambito scolastico o vietati ai minori è stato implementato un enforcing della sicurezza basato sulle seguenti tecnologie:

URL FILTERING

La Direzione Scolastica ha definito quali contenuti non rendere accessibili attraverso la rete scolastica (Es. gioco d'azzardo, pornografia). Queste categorie di siti web vengono rese

inaccessibili attraverso un motore di url filtering aggiornato via cloud, il quale cataloga e discerne i siti visitati, bloccando i contenuti proibiti.

●SSL INSPECTION

Oltre al traffico in chiaro, anche tutte le connessioni criptate eseguite da e verso la rete dell'istituto vengono analizzate dal firewall per permettere allo stesso di bloccare contenuti pericolosi o vietati ed inibire l'uso di software dannosi od il collegamento a reti o servizi maliziosi o non sicuri.

APPLICATION PROTECTION

Il firewall è in grado di discernere quali applicazioni sono in uso nei client agganciati alla rete d'istituto, per tanto è possibile inibire servizi illegali (Es. P2P) o applicazioni potenzialmente pericolose o inadatte all'ambito scolastico (Instant Messaging).

MONITORAGGIO & LOG

Qualsivoglia connessione, accesso o fruizione della rete informatica è tracciata e monitorata. Tutti i log delle attività e degli accessi vengono archiviati e sono a disposizione della dirigenza scolastica per la consultazione.

PRIVACY

I dati registrati riguardanti gli accessi ed il traffico, ed i relativi log sono anonimizzati. Qualsivoglia accesso a log contenenti dati sensibili o informazioni personali (accessi, utilizzo della rete, etc.) viene registrato e deve essere autorizzato dalla dirigente scolastica.

Art. 2 E-mail

L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. Le credenziali sono in possesso del personale amministrativo. La posta elettronica è protetta da antivirus e da antispam.

Art. 3 Blog e sito web della scuola

L'accesso al sito istituzionale non prevede un login per gli utenti e consente il collegamento al Registro Elettronico, all'Albo Pretorio e ad Amministrazione Trasparente.

Sul sito è presente un'area riservata cui ha accesso il solo personale docente tramite username e password nominali per la visualizzazione di contenuti riservati al Collegio Docenti. I docenti

sono registrati in tale area attraverso nome, cognome e indirizzo e-mail personale. Il sito è costruito con il CMS Joomla! su hosting fornito da ERGONET srl.

Art. 4 Social network

L'utilizzo dei social network nella didattica deve essere contestualizzato ad attività specifiche.

Art. 5 Protezione dei dati personali

Il trattamento dei dati personali riguarda unicamente le finalità istituzionali della scuola per le quali vengono raccolti solo i dati strettamente necessari. Essi saranno trattati con o senza l'ausilio di strumenti elettronici e comunque automatizzati secondo le modalità e le cautele previste dall'art. 13 del D.Lgs 196/2003 e conservati per il tempo necessario all'espletamento delle attività amministrative e istituzionali.

Il Regolamento Generale sul trattamento e la protezione dei dati personali è pubblicato sul sito web di istituto www.iisviagramsci.edu.it

TITOLO 4 - DEFINIZIONE DI BULLISMO E CYBERBULLISMO

Nell'ottica della prevenzione, dell'educazione, della presa di coscienza degli alunni del disvalore delle azioni poste in essere, e delle conseguenze disciplinari, è necessario inserire nel Regolamento d'Istituto un elenco delle condotte riconducibili a bullismo e a cyberbullismo

Il BULLISMO (mobbing in età evolutiva): questo è il termine di nuova generazione per indicare atti di violenza a scuola generalmente nel periodo adolescenziale e pre-adolescenziale. Esistono vari modi con cui il bullo può prevaricare la vittima, in maniera diretta o indiretta, in maniera palese o in maniera sottile. Si tratta sempre di bullismo e ognuna di queste modalità danneggia la vittima, creando disagi di varia gravità a seconda del tipo di prevaricazioni e del tipo di vittima. Bisogna precisare che nonostante a volte il bullismo psicologico venga citato come una forma a sé stante, tutte le tipologie di bullismo provocano disagi psicologici.

- **fisico**: atti aggressivi diretti (dare calci, pugni, ecc.), danneggiamento delle cose altrui, furto intenzionale. Si può parlare di bullismo fisico quando le prevaricazioni avvengono attraverso il contatto fisico, cioè quando il bullo aggredisce la vittima con: spintoni, sgambetti, schiaffi, calci, pugni, strattoni, afferrando la vittima per i vestiti, sbattendola al

muro, mettendola alle strette in un angolo, introdurla in altri luoghi con la forza, cercare di spogliarla etc.

- **verbale:** manifesto (deridere, umiliare, svalutare, criticare, accusare, ecc.) o nascosto (diffondere voci false e offensive su un compagno, provocazioni, ecc.); quindi, il bullismo verbale è quando le prevaricazioni avvengono solo ed esclusivamente attraverso il linguaggio: insulti, prese in giro, fastidiosi nomignoli, piccole minacce.
- **relazionale:** sociale (escludere il compagno dalle attività di gruppo) o manipolativo (rompere i rapporti di amicizia di cui gode la vittima).
- **sociale:** con bullismo sociale si intendono tutti i comportamenti che il bullo adotta per isolare la vittima dal gruppo dei pari, attraverso l'emarginazione, l'esclusione da gruppi e dai giochi, la diffamazione, cioè parlare male della vittima con gli altri compagni per metterla in cattiva luce. Inoltre il bullo tende ad incolpare la vittima ingiustamente di atti che non ha commesso.
- **strumentale:** per bullismo strumentale si intendono tutte quelle azioni che mirano al danneggiamento o all'appropriazione di oggetti appartenenti alla vittima.

TIPOLGIE DI CYBERBULLISMO

- **FLAMING:** Il flaming (battaglie verbali online) è una forma di cyberbullismo atipica, in quanto i messaggi elettronici, violenti e volgari, sono inviati da due contendenti che hanno lo stesso potere, che non necessariamente si frequentano nella vita reale e che si affrontano "ad armi pari", per una durata temporale delimitata dall'attività on line condivisa. Può essere utile sapere che durante la partecipazione alle chat (soprattutto le ragazze) e ai videogiochi interattivi (soprattutto i ragazzi), moltissimi preadolescenti ed adolescenti si "divertono", insultandosi reciprocamente.
- **HARASSMENT:** Dall'inglese "molestia", l'harassment consiste in messaggi insultanti e volgari che vengono inviati ripetutamente nel tempo, attraverso l'uso del computer e/o del videotelefonino. Accanto ad e-mail, sms, mms offensivi, pubblicazioni moleste su Blog e spyware per controllare i movimenti on line della vittima, le telefonate mute rappresentano sicuramente la forma di molestia più utilizzata dai cyberbulli, soprattutto nei confronti del sesso femminile.
- **CYBERSTALKING:** Quando l'harassment diviene particolarmente insistente ed intimidatorio e la vittima comincia a temere per la propria sicurezza fisica, il comportamento offensivo assume la denominazione di cyberstalking, facilmente riscontrabile nell'ambito di relazioni fortemente conflittuali con i coetanei e soprattutto nel caso di rapporti sentimentali interrotti tra pari.

- **DENIGRATION:** A differenza di quanto avviene nel cyberstalking, l'attività offensiva ed intenzionale del cyberbullo, che mira a danneggiare la reputazione e la rete amicale di un coetaneo, può concretizzarsi anche in una sola azione (esempio: pubblicare su un sito una foto ritoccata etc.) al fine di ridicolizzarlo, indire una votazione on line per screditare.
- **IMPERSONATION:** Se uno studente viola l'account di qualcuno (perché ha ottenuto consensualmente la password o perché è riuscito, con appositi programmi, ad individuarla) può, allora, farsi passare per questa persona e inviare messaggi con l'obiettivo di dare una cattiva immagine della stessa, crearle problemi o metterla in pericolo, danneggiarne la reputazione o le amicizie.
- **SEXTING:** E' l'invio di fotografie a sfondo sessuale via smartphone o altri dispositivi attraverso l'utilizzo della rete Internet, corredati da immagini a sfondo sessuale. Se dette immagini, ottenute tramite la confidenza tra due persone, viene divulgata illegittimamente in rete, si tratta di cyberbullismo.
- **EXCLUSION:** Il cyberbullo decide di escludere intenzionalmente un coetaneo da un gruppo online ("lista di amici"), da una chat, da un game interattivo o da altri ambienti protetti da password. Spesso gli studenti per indicare questa prepotenza utilizzano il termine "bannare".

TITOLO 5 - COME SEGNALARE

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, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Si potrebbero palesare 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.

Strumenti a disposizione di studenti/esse

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

- indirizzo e-mail specifico 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 e al numero gratuito [1.96.96](tel:19696) Telefono Azzurro.

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.

A tale proposito 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 (19696) è sempre attiva nell’offrire una guida competente ed 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 ed 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 e 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 degli ambulatori specificatamente 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 dovute 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.

MODULO PER LA SEGNALAZIONE

(Il presente modulo va compilato dal docente che raccoglie la segnalazione con la collaborazione dello studente)

● Episodio di:

- o Bullismo
- o Cyberbullismo
- o Sexting
- o Grooming

Alunni coinvolti:

Vittima/e _____

Responsabile/i _____

● Quando? _____

● Dove? _____

● Descrizione del fatto:

Data _____

Il docente _____

INDICE

Titolo 1 - Il documento di E-Policy	pag. 2
Introduzione	pag. 2
Art.1 Scopo dell'E-Policy	pag. 2
Art.2 Ruoli e responsabilità	pag. 3
Art.3 Informativa per i soggetti esterni che erogano attività educative nell'Istituto	pag. 4
Art.4 Condivisione e comunicazione dell'E-Policy	pag. 5
Art.5 Gestione delle infrazioni alla E-Policy.....	pag. 5
Art.6 Monitoraggio dell'implementazione della Policy e suo aggiornamento	pag. 7
Art.7 Integrazione della Policy con regolamenti esistenti	pag. 7
Titolo 2 - Formazione e curriculum	pag. 8
Art.1 Curriculum sulle competenze digitali per gli studenti	pag. 8
Art.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica e sull'uso consapevole di Internet e delle tecnologia digitali	pag. 8
Art.3 Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità	pag. 8
Titolo 3 - Gestione dell'infrastruttura e della strumentazione ICT della e nella scuola	pag. 9
Art.1 Accesso ad Internet e Gestione accessi (password)	pag. 9
Art.2 E-mail	pag. 10
Art.3 Blog e sito web della scuola	pag. 11
Art.4 Social network.....	pag.11

Art.5 Protezione dei dati personali.....	pag.11
Titolo 4 - Definizione di bullismo e cyberbullismo.....	pag. 11
Il bullismo	pag. 11
Tipologie di cyberbullismo	pag. 12
Titolo 5 - Come segnalare	pag. 13
Strumenti a disposizione di studenti/esse	pag. 14
Attori sul territorio	pag. 14
Allegato 1	pag. 16