Documento di ePolicy

RMPC080007

L.G.S "ENNIO QUIRINO VISCONTI"

PIAZZA DEL COLLEGIO ROMANO 4 - 00186 - ROMA - ROMA (RM)

Rita Pappalardo

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse.

Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

In un contesto sempre più complesso, diventa 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, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

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

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico; le misure per la prevenzione e la sensibilizzazione 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.

Argomenti del Documento

Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

1.2 - 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, s'impegni nell'attuazione e promozione di essa.

Il Dirigente Scolastico

il Dirigente Scolastico garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica. E' quindi importante, che sia formato adeguatamente sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIUR; promuove, inoltre, la cultura della sicurezza online e dà il proprio contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC. Il Dirigente Scolastico ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

L'Animatore digitale

l'Animatore digitale supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale"; monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola, e, attraverso la gestione della piattaforma e in collaborazione con il tecnico esterno e il tecnico interno controlla che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

Il Referente bullismo e cyberbullismo

"Ogni Istituto scolastico, nell'ambito della propria autonomia, individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo" (Art. 4 Legge n.71/2017, "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo" (permalink – file 1 LEGGE 71_2017 in allegato). Questa figura ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Si adopera per coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.

I Docenti

i Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. E' opportuno che integrino parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica. I docenti accompagnano e supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici 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 e Ausiliario (ATA)

il personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il Dirigente Scolastico e con il personale docente tutto. Diverse figure che, in sinergia, si occupano ciascuno per la propria funzione, del funzionamento dell'Istituto scolastico che passa anche attraverso lo sviluppo della cultura digitale e dell'organizzazione del tempo scuola. Il personale ATA è concretamente coinvolto nell'applicazione della legge 107/15 ("La Buona Scuola") che concerne non solo il tempo scuola e il potenziamento dell'offerta formativa, ma anche le attività di formazione e autoformazione in tema di bullismo e cyberbullismo. Il personale ATA è coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo.

Gli Studenti e le Studentesse

gli Studenti e le Studentesse devono, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola devono imparare a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le; devono partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete.

I Genitori

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

Gli Enti educativi esterni e le associazioni

gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola devono conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC, a tale scopo è stata redatta una informativa.

1.3 - Un'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 di 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).

Tutti i soggetti esterni coinvolti nelle attività della scuola, sono tenuti a leggere il Documento e-policy e i regolamenti di Istituto.

Dotarsi di un'informativa sintetica sull'ePolicy comprensiva delle procedure di segnalazione da condividere con tutte le figure che operano con studenti e studentesse, significa non solo tutelare questi ultimi e la scuola stessa, ma anche porre in essere nuove modalità per rilevare, limitare e contrastare possibili pericoli legati a condotte educative non professionali.

Il Documento permette di tutelare ragazzi e ragazze da comportamenti potenzialmente rischiosi messi in atto da soggetti esterni alla scuola e che si trovano ad operare all'interno dell'Istituto.

In coerenza con il percorso intrapreso la Scuola ha previsto una informativa e-policy specifica per i soggetti esterni:

DOCUMENTO E-POLICY ENTI ESTERNI

Gli Enti educativi esterni e le associazioni che entrano in relazione con la Scuola, in particolare per i PCTO o per Progetti di ampliamento dell'offerta formativa, devono conformarsi alla politica del Liceo Visconti riguardo all'uso consapevole della Rete e delle TIC; devono promuovere comportamenti sicuri, vigilare sulla sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme. In genere gli Enti esterni accolgono la partecipazione degli studenti alle attività da loro gestite utilizzando un indirizzo e-mail privato dello studente, gli account all'interno del dominio "liceoeqvisconti.it" sono infatti protetti e non sono abilitati a comunicare all'esterno del dominio; si tratta di uno strumento di sicurezza ma anche di libertà e responsabilità, lo studente infatti potrebbe avere di nuovo rapporti con l'Ente esterno dopo la conclusione del corso di studi, quando l'account del dominio della Scuola viene eliminato. Una liberatoria in tal senso sarà quindi inserita nel Patto Formativo previsto per i PCTO e/o sarà richiesta dall'Ente esterno alle famiglie degli studenti all'atto di iscrizione all'attività. Gli Enti esterni saranno corresponsabili, nel caso in cui vi sia la partecipazione diretta di un docente della scuola, o responsabili, nel caso non vi sia partecipazione diretta di un docente, della sicurezza nell'uso della Rete e delle TIC. In caso di eventuali problemi o violazione delle Norme, il Responsabile dell'Ente esterno invierà tempestivamente una segnalazione al Dirigente Scolastico e, a seconda dei casi, al Referente per il bullismo, al Referente E-Policy, all'Animatore Digitale. Anche le famiglie sono tenute a

collaborare per l'uso corretto, responsabile e consapevole della Rete e delle TIC, nelle attività che coinvolgono Enti esterni, allo stesso modo in cui lo sono nelle attività didattiche.

Qualora si verifichino episodi che mettano in pericolo studenti e studentesse l'ente esterno è tenuto ad informare tempestivamente, con le modalità previste dai regolamenti, il Dirigente Scolastico, il referente e-policy, il referente bullisomo e cyberbullismo

---

1.4 - Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

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/lle 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 Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'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.

Il Patto di corresponsabilità della scuola sarà aggiornato in questo senso nel settembre 2022.

Il documento E-Policy del Liceo Visconti, pubblicato per la prima volta nel novembre 2021, a cura del Gruppo E-Policy, sarà approvato dal Collegio dei Docenti e dal

Consiglio di Istituto. Eventuali modifiche proposte dalle diverse componenti della comunità scolastica saranno inserite nel 2022.

1.5 - Gestione delle infrazioni alla ePolicy

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

Possibili condotte sanzionabili, in relazione all'uso improprio delle TIC e della Rete a scuola da parte degli studenti e delle studentesse, saranno esaminate, valutate ed eventualmente sanzionate a cura del Dirigente Scolastico, del Referente E-Policy e del Referente bullismo e cyber-bullismo. A seconda dell'età dello studente o della studentessa, si interverrà su tutto il contesto classe, con attività specifiche educative e di sensibilizzazione, allo scopo di promuovere una maggior consapevolezza circa l'utilizzo delle TIC e di Internet. Si valuterà inoltre la natura e la gravità di quanto accaduto, al fine di considerare la eventuale necessità di denunciare l'episodio (con il coinvolgimento ad es. della Polizia Postale) o di limitarsi a garantire immediato supporto psicologico allo/la studente/ssa attraverso i servizi predisposti.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

Un aggiornamento specifico del Patto di Corresponsabilità e del Regolamento di Istituto, con riferimenti alla E-Policy verrà completato nel corso dell'a.s. 2021/2022.

1.7 - Monitoraggio

dell'implementazione della ePolicy e suo aggiornamento

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

Poiché il Liceo Visconti si dota per la prima volta del Documento E-Policy, aggiornamenti e modifiche, eventualmente proposti da tutte le componenti della comunità scolastica, saranno valutate e discusse nel corso dell'anno scolastico

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare uno o più eventi o attività di presentazione del progetto Generazioni Connesse a docenti, studenti e genitori.
- Curare la diffusione del Documento e-policy e delle integrazioni ai Regolamenti di Istituto
- Prevedere una minima formazione di base per i docenti

Azioni da svolgere nei prossimi 3 anni:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare le componenti dell'Istituto per una eventuale revisione dell'ePolicy.
- Organizzare attività di monitoraggio e verifica del progetto ePolicy.
- Organizzare eventi periodici di presentazione del progetto Generazioni Connesse.
- Organizzare eventi periodici di presentazione e conoscenza dell'ePolicy.

2021/2022.

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

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

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

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale.

Curriculum digitale per gli studenti

1. IV Ginnasio – alfabetizzazione I livello: casella di posta nel dominio "liceoeqvisconti.it"; uso della password, uso della casella di posta, allegati, Drive (3 tipologie); netiquette di base; pratica dei Tutorial per il corretto uso di Classroom – E-Policy – indicazioni fondamentali sulla piattaforma "Generazioni connesse", > a cura del Gruppo E-Policy e in particolare del Referente per il bullismo e cyberbullismo, almeno un incontro illustrativo, a cura del referente e/o di docenti della classe illustrazione, discussione, verifica relativa ad alcuni tra gli argomenti previsti nella Formazione di Generazioni connesse.
2. V Ginnasio – alfabetizzazione II livello: ripresa contenuti IV Ginnasio + approfondimento; uso di Classroom; creazione e condivisione dei documenti utilizzando Google Doc, Google Fogli, Google Presentazioni; netiquette – E-Policy – iscrizione alla piattaforma "Generazioni connesse", > a cura del

Gruppo E-Policy e in particolare del Referente per il bullismo e cyberbullismo, almeno un incontro illustrativo, a cura del referente e/o di docenti della classe, partecipazione alla formazione on line, con attestato agli Atti della Scuola; conoscenze di base per una corretta ricerca in rete.

3. I, II e III Liceo – Sviluppo di specifiche competenze (almeno due per anno di corso), individuate tra quelle comprese nell'elenco allegato, scelte sulla base della programmazione del Consiglio di Classe e dei singoli docenti disponibili a sviluppare l'attività (AD e Docenti del Team saranno disponibili per sostenere il lavoro dei colleghi; nel caso in cui in un Consiglio di Classe non vi sia alcun docente disponibile, interverrà direttamente uno dei Docenti del Team) – per tutti >E-Policy – iscrizione alla piattaforma "Generazioni connesse" (per chi non lo avesse già fatto), > a cura del Referente e/o di docenti della classe, partecipazione alla formazione on line, con attestato agli Atti della Scuola.

Il Curriculum sarà avviato per le classi ginnasiali nel corrente anno scolastico, dopo l'inserimento nel nuovo PTOF 2022/25 entrerà a regime per tutte le classi.

2.2 - Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

Le TIC, infatti, dovrebbero essere usate dagli insegnanti ad integrazione della didattica al fine di progettare, sviluppare, utilizzare, gestire e valutare i processi di insegnamento e apprendimento di tutti gli studenti e le studentesse della classe, anche delle persone con disabilità (in chiave inclusiva). Di conseguenza, gli insegnanti dovrebbero avere o raggiungere un buon livello di formazione in merito all'utilizzo e l'integrazione delle TIC nella didattica, tenendo presente l'immagine che fornisce in merito il DigComp: "imparare a nuotare nell'oceano digitale". È su tali premesse che l'Istituto, attraverso il Collegio dei Docenti, ha riconosciuto e favoritola partecipazione del personale ad iniziative promosse sia direttamente dalla scuola (con l'aiuto dell'Animatore Digitale e del Team Digitale) dalle reti di scuole e dall'amministrazione,

sia quelle liberamente scelte dai docenti (anche online), purché restino coerenti con il piano di formazione.

L'attenzione all'uso delle TIC è fondamentale nella didattica: un loro utilizzo strutturato e integrato non solo può rendere gli apprendimenti motivanti, coinvolgenti ed inclusivi, ma permette al docente di guidare studenti e studentesse rispetto alla fruizione dei contenuti online, ormai la modalità naturale di apprendimento al di fuori della scuola. Inoltre, permettono di sviluppare capacità che sono sempre più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza e il confronto fra pari in modalità asincrona.

Dal 2016 sono stati organizzati nell'Istituto corsi di formazione per i docenti sull'utilizzo e l'integrazione delle TIC nella didattica. Anche nell'a.s. 2021/2022 saranno erogati dei corsi nei quali verrà inserita una specifica sezione dedicata all'E-Policy.

Argomenti dei corsi già erogati (in diverse edizioni)

Corso G-Suite base,

Corso presentazioni umanistiche,

Corso presentazioni scientifiche,

Corso Google Workspace avanzato,

Corso produzione audio e video.

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

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

territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

L'Istituto ha previsto un primo specifico intervento di informazione/formazione sulla e-policy e sulla piattaforma Generazione Connesse per il mese di dicembre, contenuti relativi alla E-Policy saranno inseriti nei corsi di formazionne per l'uso delle TIC programmati nel secondo periodo dell'a.s., saranno favoriti percorsi di autoaggiornamento personale.

Verrà predisposta una sezione specifica, all'interno dell'area PNSD sul Sito web dell'Istituto, ove sarà disponibile il link al progetto "Generazioni connesse" e quindi alla apposita sezione di formazione.

2.4. - 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 e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie 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.

Ci si adopererà per attuare quanto previsto nel testo standard del Documento.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022)

Scegliere almeno 1 di queste azioni

- Coinvolgere il corpo docente nella consultazione e nell'utilizzo della piattaforma "Generazioni connesse" per relaizzare sempre meglio un utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Coinvolgere i genitori, attraverso l'informazione disponibile sul sito web e opportuni avvisi nella conoscenza e consultazione dei materiali disponibili sulla piattaforma "Generazioni connesse".
- Organizzare e promuovere per il corpo docente interventi formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi)

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare e promuovere per il corpo docente interventi formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente interventi formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.

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

3.1 - Protezione dei dati personali

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

(cfr. http://www.garanteprivacy.it/scuola).

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

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8), tutelato dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

Anche le scuole, quindi, hanno oggi l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, entrato in vigore lo scorso 19 settembre.

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare

riferimento all'uso delle tecnologie digitali, e indichiamo le misure che la scuola intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori. A tal fine, l'Istituto allega alla presente ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali.

La scuola comunica (tramite apposita informativa) agli interessati le caratteristiche e modalità del trattamento dei loro dati, indicando i responsabili del trattamento.

La scuola ha adottato idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti: in particolare

- Il sito è migrato al suffisso edu.it
- Il sito sarà progettato secondo i concetti di privacy by default e by design
- è stato utilizzato il protocollo HTTPS
- è stato utilizzato un sistema di cifratura quando il trattamento dati lo richiede
- è presente un sistema di backup
- è presente un piano di disaster recovery

Per quanto riguarda la sicurezza della rete internet scolastica il personale interno ed esterno è adeguatamente qualificato e sono stati messi in atto gli strumenti previsti dalla normativa.

3.2 - Accesso ad Internet

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

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola".

Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

Tutto l'Istituto è connesso alla rete; in tutte le aule sono disponibili computer e LIM; il Liceo dispone di un dominio "liceoeqvisconti.it"; tutto il personale, docente e non docente, e tutti gli studenti sono dotati di un account all'interno del dominio. Gli account per il personale permettono di interagire sia all'interno che all'esterno del dominio, gli account-studente invece interagiscono solo all'interno del dominio.

Le famiglie vengono informate delle funzionalità dell'account-studente, firmano apposita liberatoria; le credenziali di accesso per gli studenti vengono comunicate tramite la famiglia.

3.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

E' importante effettuare una distinzione preliminare fra comunicazione interna e comunicazione esterna. Diversi strumenti di comunicazione online possono essere utilizzati dalla scuola, sia per raggiungere target esterni, al fine di valorizzare e promuovere le attività portate avanti dall'Istituto, sia per far circolare all'interno della scuola informazioni di servizio o contenuti importanti.

I principali strumenti di comunicazione esterna del Liceo Visconti, sono il sito web della scuola e il sito web della biblioteca.

Gli strumenti di comunicazione interna sono: il registro elettronico con tutte le sue funzionalità: la piattaforma Google Workspace con tutte le sue funzionalità.

Il registro elettronico permette di gestire la comunicazione con le famiglie, le quali attraverso di esso possono visualizzare molte informazioni utili, interagendo con la scuola, su:

- andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari);
- risultati scolastici (voti, documenti di valutazione);
- colloqui con le famiglie (prenotazioni individuali);
- eventi (agenda eventi);
- comunicazione varie (comunicazioni di classe, comunicazioni personali).

Le modalità e la regolamentazione per l'uso del registro elettronico sono previste dai regolamenti interni; per tutte le componenti sono disponibili manuali prodotti dal gestore del registro elettronico e specifici tutorial prodotti dall'Animatore Digitale. Per l'utilizzo della piattaforma Google Workspace la scuola ha predisposto specifici regolamenti.

Animatore Digitale e docenti del Team Digitale sono costantemente disponibili per sostenere tutte le componenti della scuola.

Per un eventuale uso delle chat in ambito scolastico (con colleghi, studenti o genitori) è bene tenere presenti alcuni consigli:

- Mettere in chiaro fin dall'inizio, comprendere e rispettare sempre le finalità del gruppo, scrivendo e pubblicando solo contenuti pertinenti a tali finalità; Usare sempre un linguaggio adeguato e il più possibile chiaro e preciso (la comunicazione online si presta spesso a non pochi fraintendimenti);
- Evitare di affrontare in chat argomenti che possano mettere in discussione il rispetto della privacy o argomenti controversi (la comunicazione online in una chat di gruppo non è adatta per la gestione di problematiche di questo tipo, che certamente è più opportuno affrontare in presenza o in un Consiglio di classe);
- Evitare discussioni di questioni che coinvolgono due o pochi interlocutori, onde evitare di annoiare e disturbare gli altri componenti del gruppo;
- Non condividere file multimediali troppo pesanti;
- Evitare assolutamente di condividere foto di persone (studenti, docenti, personale della scuola) in chat;

- Indirizzare solo domande precise e chiare, a cui si possano dare risposte altrettanto brevi e precise;
- Evitare messaggi troppo spezzettati, cercando il più possibile di essere brevi ed esaustivi allo stesso tempo;
- nel caso di interazione docente/studente chiedere e raccogliere apposita liberatoria da parte della famiglia.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

La presente ***ePolicy*** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

Come previsto dal Regolamento per l'uso della Piattaforma Google Workspace (ex Google Suite), l'uso del BYOD è incoraggiato, sulla base di quanto previsto dal PNSD e dalle indicazioni del Ministero dell'Istruzione, ma sempre strettamente nei limiti delle indicazioni del docente che ne propone l'utilizzo.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022).

- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali e sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali e sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a informare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali e sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto perredigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali e sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali e sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a informare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali e sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

Capitolo 4 - Rischi on line: conoscere, prevenire e rilevare

4.1 - Sensibilizzazione e Prevenzione

Il rischio online si configura come la possibilità per il minore di:

- commettere azioni online che possano danneggiare se stessi o altri;
- essere una vittima di queste azioni;
- osservare altri commettere queste azioni.

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

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

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

Gli interventi di sensibilizzazione sono volti a:

- accrescere la consapevolezza in tutta la comunità scolastica relativamente a tutti gli aspetti della E-Policy;
- incoraggiare tutte le componenti (docenti, non docenti, studenti e famiglie) a

- modificare i propri comportamenti rendendoli più funzionali;
  favorire la diffusione di informazioni e servizi disponibili all'utilità collettiva per la conoscenza dell'ePolicy.

Affinché la sensibilizzazione sia efficace, è importante che sia chiara l'azione verso cui i soggetti devono impegnarsi. Due sono gli aspetti che bisogna tenere in considerazione:

- la consapevolezza dello status quo;
- la motivazione al cambiamento.

Interventi di prevenzione

La prevenzione in ambito digitale consiste in azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati ad esse, per la sicurezza di ragazze/i.

Il problema della "sicurezza" deve essere preferibilmente gestito attraverso la prevenzione. Le dimensioni che il fenomeno coinvolge sono molteplici e non puramente tecniche e si rifanno alla capacità dei più giovani di gestire situazioni complesse che richiedono: la capacità di gestire la relazione con l'altro/a diverso/a da sé; le dimensioni dell'affettività e della sessualità; il riconoscimento di un limite, anche, ma non solo, legato ad una dimensione di legalità; l'utilizzo sicuro e consapevole delle tecnologie digitali.

La scuola deve rafforzare la sua capacità di rispondere a questi bisogni attraverso strumenti e misure specifiche. Quando un evento problematico connesso ai rischi online coinvolge il contesto scolastico, è fondamentale per la scuola poter dare una risposta il più possibile integrata, che trovi la sua espressione di indirizzo in procedure chiare di cui deve dotarsi e che includano la collaborazione (prevedendo accordi specifici) con la rete dei servizi locali (in primis le ASL e la Polizia Postale).

La responsabilità dell'azione preventiva ed educativa chiama in campo diverse componenti educative oltre alla scuola, come la famiglia, ma non solo (istituzioni, associazioni, società civile, etc.), ciascuna con un proprio compito nei confronti degli adolescenti. Tali agenzie sono chiamate a collaborare ad un progetto comune, nell'ambito di funzioni educative condivise. La necessità di questa collaborazione nasce, più o meno consapevolmente, dal riconoscimento, sia da parte dei genitori che da parte degli insegnanti, della rispettiva difficoltà a svolgere, da soli, la propria funzione formativa ed educativa in ambito digitale. Questo anche a causa della continua evoluzione delle competenze che le tecnologie digitali richiedono. La necessità di supportare un uso positivo e consapevole delle TIC da parte dei più giovani, sia in un'ottica di tutela dai rischi potenziali che nella valorizzazione delle opportunità esistenti, pone la scuola e i genitori di fronte alla sfida di riconsiderare la propria identità, il proprio ruolo educativo e le proprie risorse, oltre allo stato dei rapporti reciproci per un patto educativo da rinnovare costantemente.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

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

La stessa legge e le relative **Linee di orientamento per la prevenzione e il contrasto del cyberbullismo** indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.

Nomina del Referente per le iniziative di prevenzione e contrasto che:

- Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
- Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Il cyberbullismo è una forma di prepotenza virtuale messa in atto attraverso l'uso di Internet e delle tecnologie digitali. Spesso i termini bullismo e cyberbullismo vengono usati impropriamente e si riconducono ad essi i più svariati episodi di violenza o offese

fra ragazzi/e. Bullismo e cyberbullismo hanno, però, connotati ben precisi e non vanno confusi con altre problematiche del mondo giovanile.

Nel 2006 Smith e collaboratori definirono il cyberbullismo come:

“Un atto aggressivo e intenzionale perpetrato da un individuo o da un gruppo, attraverso l’uso delle nuove tecnologie della comunicazione, in modo ripetuto e continuato nel tempo, contro una vittima che non può facilmente difendersi” (in Smith P.K., Mahdavi J., Carvalho C., e Tippett N., An investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbullying. A Report to the Anti-Bullying Alliance, 2006, p.6).

Mentre nel bullismo tradizionale il potere presenta connotati ben precisi, potrebbe essere, ad esempio, di tipo fisico (legato alla forza o alla statura) o sociale (legato alla popolarità), il potere online può derivare semplicemente dal possesso di specifiche competenze o di alcuni contenuti (immagini, video, confessioni) che potrebbero essere utilizzati per danneggiare la vittima.

Solitamente, quando si parla di cyberbullismo o di bullismo si intende che vittima e bullo/cyberbullo siano minori o comunque adolescenti (sono esclusi, quindi, dalla definizione episodi di prevaricazione che avvengono fra adulti o fra un adulto e un minore). Il cyberbullo non è mai totalmente consapevole delle conseguenze delle proprie azioni. L’impossibilità di vedere con i propri occhi l’eventuale sofferenza e umiliazione provata dalla vittima, fa sì che il tutto venga percepito come “uno scherzo” divertente a cui partecipare, di cui ridere o a cui essere indifferenti. Inoltre, il cyberbullismo non lascia segni fisici evidenti sulla vittima e si consuma in un contesto virtuale che spesso viene percepito dai ragazzi come non “reale”, come un mondo ludico a sé stante. La mediazione tecnologica, infatti, porta ad un certo distanziamento fra aggressore e vittima, causando quello che Bandura ha definito come “disimpegno morale”. Si tratta di un indebolimento del controllo morale interno dell’individuo, con la conseguente minimizzazione delle responsabilità individuali. Tale fenomeno vale non solo per il cyberbullo, ma anche per i cosiddetti bystander, ossia coloro che sono spettatori dei fatti.

Ad aggravare il fenomeno contribuiscono convinzioni o tendenze frequenti nell’uso della Rete, sia da parte dei giovani che degli adulti:

- Percezione che online non ci siano norme sociali da rispettare;
- Falsa convinzione secondo cui la Rete sia uno spazio virtuale lontano dalla realtà, in cui vige libertà assoluta;
- Possibilità di sperimentare online identità e personalità multiple “fingendo di essere ciò che non si è”;
- Attitudine a vivere Il contesto virtuale come un luogo di simulazione e giochi di ruolo;
- Dispersione della responsabilità: tutti quelli che partecipano anche solo con un like o un commento diventano, di fatto, corresponsabili delle azioni del

cyberbullo aumentando la portata dell'azione; mettere un "like" su un social network commentare o condividere una foto o un video che prende di mira qualcuno o semplicemente tacere pur sapendo, mette ragazzi e ragazze nella condizione di avere una responsabilità.

Il gruppo "silente" che partecipa senza assumersi la responsabilità, rappresenta, in realtà, anche l'elemento che può fermare una situazione di cyberbullismo.

È possibile suddividere gli atti di cyberbullismo in due grandi gruppi:

cyberbullismo diretto: il bullo utilizza strumenti di messaggistica istantanea (es. sms, whatsapp) che hanno un effetto immediato sulla vittima, poiché inviati direttamente.

cyberbullismo indiretto: il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatorii per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima anche da un punto di vista psicologico.

Il cyberbullismo è una problematica che non riguarda unicamente vittima e cyberbullo. È un fenomeno sociale e di gruppo, centrale è il ruolo di: famiglia, scuola, media, tecnologie digitali e gruppo dei pari.

Chi compie atti di bullismo e cyberbullismo può anche essere responsabile di reati penali e danni civili.Secondo il codice penale italiano i comportamenti penalmente rilevanti in questi casi sono:

percosse (art. 581),

lesione personale (art. 582),

ingiuria (art. 594),

diffamazione (art. 595),

violenza privata (art. 610),

minaccia (art. 612),

danneggiamento (art. 635).

Quali sono le responsabilità dei genitori e dei docenti/educatori?

L'atto di bullismo può violare sia la legge penale, sia quella civile, quindi può dar vita a due processi, l'uno penale e l'altro civile.

Le responsabilità per atti di bullismo e cyberbullismo compiute dal minorenne possono ricadere anche su:

- I genitori, perché devono educare adeguatamente e vigilare, in maniera adeguata all'età del figlio, cercando di correggerne comportamenti devianti. Questa responsabilità generale persiste anche per gli atti compiuti nei tempi di affidamento alla scuola (culpa in educando).
- Gli insegnanti e la scuola: perché nei periodi in cui il minore viene affidato all'Istituzione scolastica il docente è responsabile della vigilanza sulle sue azioni e ha il dovere di impedire comportamenti dannosi verso gli altri/e ragazzi/e, insegnanti e personale scolastico o verso le strutture della scuola stessa. A pagare in primis sarà la scuola, che poi potrà rivalersi sul singolo insegnante. La responsabilità si estende anche a viaggi, gite scolastiche, manifestazioni sportive organizzate dalla scuola (culpa in vigilando).
- Esiste poi una culpa in organizzando, che si ha quando la scuola non mette in atto le azioni previste per la prevenzione del fenomeno o per affrontarlo al meglio (così come previsto anche dalla normativa vigente).

Per quanto riguarda la responsabilità dei docenti va considerato tutto il tempo dell'affidamento dell'alunno alla scuola. Quindi, non soltanto le ore delle attività didattiche, ma anche tutti gli altri momenti della vita scolastica, compresa la ricreazione, la pausa pranzo, la palestra, le uscite e i viaggi di istruzione etc.

Il Liceo Visconti ha, già da qualche anno provveduto, a nominare un Referente per Bullismo e Cyberbullismo, partendo dalla elaborazione e pubblicazione di questo Documento E-Policy, intende aggiornare i Regolamenti esistenti e prevedere attività volte alla formazione di docenti e studenti e alla informazione delle famiglie.

In ottemperanza alla Legge 71/2017 e alle relative "Linee di orientamento per la prevenzione e il contrasto del cyberbullismo" le linee di azione previste dall'Istituto sono:

- formazione del personale scolastico;
- sviluppo delle competenze digitali;
- promozione di un ruolo attivo degli studenti in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti.

Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
Il Referente per Bullismo e Cyberbullismo:

- Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
- Svolge un importante compito di supporto nei confronti del Dirigente Scolastico

Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza. Per quanto riguarda la necessità di segnalazione e rimozione, ciascun

minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore. Il Garante ha pubblicato nel proprio sito un apposito modello per la segnalazione/reclamo in materia di cyberbullismo, da inviare a: cyberbullismo@gpdp.it.

Parallelamente, nel caso in cui si ipotizzi che ci si possa trovare di fronte ad una fattispecie di reato (come, ad esempio, il furto di identità o la persistenza di una condotta persecutoria che mette seriamente a rischio il benessere psicofisico del bambino/a o adolescente coinvolto/a in qualità di vittima) si potrà far riferimento agli uffici preposti delle Forze di Polizia per inoltrare la segnalazione o denuncia/querela e permettere alle autorità competenti l'approfondimento della situazione da un punto di vista investigativo. È in tal senso possibile far riferimento a questi uffici: Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato – Commissariato on line (attraverso il portale http:// www.commissariatodips.it).

Per un consiglio e un supporto è possibile rivolgersi alla Helpline di Telefono Azzurro per Generazioni Connesse: operatori esperti e preparati sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che degli adolescenti, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti l'utilizzo dei media digitali.

4.3 - Hate speech: che cos'è e come prevenirlo

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

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

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

Come riconoscerlo e prevenirlo

Il discorso d'odio procura sofferenza. La parola ferisce, e a maggior ragione l'odio! Il discorso può violare i diritti umani. Il discorso d'odio online non è meno grave della sua espressione offline, ma è più difficile da individuare e da combattere.

Gli atteggiamenti alimentano gli atti. Il discorso dell'odio è pericoloso anche perché può condurre a più gravi violazioni dei diritti umani, e perfino alla violenza fisica. Può contribuire a inasprire le tensioni razziali e altre forme di discriminazione e di violenza.

L'odio online non è solo espresso a parole. Internet ci permette di comunicare rapidamente e in modi svariati, ad esempio, mediante i social media e i giochi online, molto spesso, d'altronde, in maniera anonima. L'odio online può esprimersi sotto forma di video e foto, come pure, più solitamente, di contenuto testuale. Le forme visive o multimediali hanno sovente un impatto più forte sugli atteggiamenti (consci e inconsci).

L'odio prende di mira sia gli individui che i gruppi. L'odio online può prendere di mira dei gruppi che spesso sono già vulnerabili sotto altri aspetti, come i richiedenti asilo, le minoranze religiose o le persone con disabilità. Tuttavia, anche i singoli individui sono sempre maggiormente oggetto di attacchi. Le conseguenze sono talvolta fatali, come dimostrato da numerosi fatti di cronaca riferiti dai media, riguardanti giovani vittime di cyberbullismo che sono state spinte al suicidio.

Internet è difficilmente controllabile. La diffusione di messaggi di incitamento all'odio è sottoposta a minori controlli. È più facile (e comporta meno rischi) insultare o molestare online, perché le persone spesso si esprimono sotto la copertura dell'anonimato.

Gli atteggiamenti e le tensioni sociali che suscitano sentimenti di odio online affondano le loro radici nella società, e non sono diversi, in genere, da quelli che alimentano il discorso dell'odio offline.

Le due presunte caratteristiche delle interazioni sociali in rete sono: l'impunità e l'anonimato. Queste abbassano le remore etiche. In realtà, però, qualsiasi azione compiuta sul web consente di rintracciare il suo autore.

Come riconoscerlo?

Il discorso dell'odio si manifesta con un ampio spettro di azioni: sebbene tutte le espressioni che istigano all'odio meritino di essere classificate come malvagie, ne esistono alcune che possono essere peggiori di altre. È utile, quindi, prendere in considerazione alcuni aspetti:

- Il contenuto e il tono
- L'intenzione degli autori degli insulti
- I bersagli o i bersagli potenziali
- Il contesto
- L'impatto o l'impatto potenziale

Come intervenire?

Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete.

Occorre in tal senso fornire ai più giovani gli strumenti necessari per decodificare gli stereotipi su cui spesso si fondano forme di hate speech, e promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network.

Si potrebbe, quindi, pensare ad attività di analisi e produzione mediale, finalizzate soprattutto a:

- fornire agli studenti gli strumenti necessari per decodificare gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire interventi comunicativi consapevoli e costruttivi da parte dei giovani.

4.4 - Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale?

Nel Liceo Visconti non si sono rilevati, almeno fino ad ora particolari situazioni di dipendenza da Internet e Gioco on line, tuttavia poiché la tecnologia ha modificato gli ambienti che viviamo e ha un impatto sulla qualità della vita, in tutti gli interventi di formazione e informazione previsti si cureranno gli elementi che contribuiscono al benessere digitale:

- la ricerca di equilibrio nelle relazioni online
- l'uso degli strumenti digitali per il raggiungimento di obiettivi personali
- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile
- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche)

Si tratta di un argomento trasversale, che coinvolge la cittadinanza digitale; è importante fare in modo che, per studentesse e studenti, la tecnologia sia strumento per raggiungere i propri obiettivi e non sia solo distrazione o addirittura ostacolo.

La scuola può insegnare molto da questo punto di vista se integra la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online.

4.5 - Sexting

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

Le caratteristiche del fenomeno sono principalmente:

- la fiducia tradita: chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo, inoltre, alla motivazione della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale);

- la pervasività con cui si diffondono i contenuti: in pochi istanti e attraverso una condivisione che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso a un numero esponenziale e infinito di persone e ad altrettante piattaforme differenti. Il contenuto, così, diventa facilmente modificabile, scaricabile e condivisibile e la sua trasmissione è incontrollabile; la persistenza
- del fenomeno: il materiale pubblicato online può permanervi per un tempo illimitato e potrebbe non essere mai definitivamente rimosso. Un contenuto ricevuto, infatti, può essere salvato, a sua volta re-inoltrato oppure condiviso su piattaforme diverse da quelle originarie e/o in epoche successive.

La consapevolezza, o comunque la sola idea di diffusione di contenuti personali, si replica nel tempo e può finire con il danneggiare, sia in termini psicologici che sociali, sia il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che hanno contribuito a diffonderla. Due agiti, quindi, che sono fra loro strettamente legati e che rappresentano veri e propri comportamenti criminali i quali hanno ripercussioni negative sulla vittima in termini di autostima, di credibilità, di reputazione sociale off e on line. A ciò si associano altri comportamenti a rischio, di tipo sessuale ma anche riferibili ad abuso di sostanze o di alcool.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/i e depressione.

4.6 - Adescamento online

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

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di***teen dating*** (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies – l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

Le fasi dell'adescamento. Il processo di adescamento segue generalmente 5 fasi:

1. Fase dell'amicizia iniziale: Questa è la fase in cui l'adescatore cerca i primi contatti con la vittima individuata, provando a socializzare con lei. Tenterà, quindi, di conoscerla meglio al fine di scoprirne bisogni, interessi e il contesto in cui vive. Condividendo argomenti di interesse del minore l'adescatore cercherà pian piano di conquistarsi la sua fiducia, ponendogli domande frequenti che attestano interesse e attenzione nei suoi confronti. Gradualmente affronterà con la vittima argomenti sempre più privati ed intimi.
2. La fase di risk-assessment: in seguito ai primi contatti con il minore, l'adescatore cerca di comprendere il contesto in cui si svolge l'interazione (es. da dove si collega alla Rete? I genitori lo controllano quando chatta? Che rapporto ha con loro?). L'obiettivo dell'adescatore è quello di rendere sempre più privato ed "esclusivo" il rapporto, cercando di passare, ad esempio, da una chat pubblica ad una privata, da una chat alle conversazioni attraverso il telefono, per poterne così carpire il numero.
3. Fase della costruzione del rapporto di fiducia: le confidenze e le tematiche affrontate divengono via via più private ed intime o comunque molto personali. In questa fase l'adescatore può iniziare a fare regali di vario tipo alla vittima e può anche avvenire lo scambio di foto, subito e non necessariamente a sfondo sessuale.
4. Fase dell'esclusività: l'adescatore rende la relazione con il minore sempre più "segreta", isolandolo sempre più dalla famiglia e dagli amici. Chiederà alla vittima di non raccontare a nessuno ciò che sta vivendo. L'esperienza reciproca verrà presentata come un "geloso segreto" da custodire per non rovinare tutto. In questa fase l'adescatore potrà ricorrere a ricatti morali puntando sulla fiducia costruita, sulla paura o sul senso di colpa.
5. Fase della relazione sessualizzata: in questa fase la richiesta di immagini o video sempre più privati e a sfondo erotico potrebbe essere più insistente, così come la proposta di incontri offline. Qualora il minore avesse già inviato immagini o video privati, potrebbe essere ricattato dall'adescatore: se non accettasse un eventuale incontro l'adescatore potrebbe diffondere quel materiale online. Questi, inoltre, tenderà a presentare sempre la situazione come "normale" al fine di vincere le eventuali resistenze del minore a coinvolgersi in tale rapporto.

Per riconoscere un eventuale caso di adescamento online è importante prestare attenzione a piccoli segnali che possono essere indicatori importanti, come ad esempio un cambiamento improvviso nel comportamento di un minore, ad esempio:

- Il minore ha conoscenze sessuali non adeguate alla sua età?
- Venite a conoscenza di un certo video o di una foto che circola online o che il

- minore ha ricevuto o filmato, ma c'è imbarazzo e preoccupazione nel
- raccontarvi di più...
  Il minore si isola totalmente e sembra preso solo da una relazione online?
  Ci sono prese in giro e allusioni sessuali verso un bambino/ragazzo in particolare?

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

Il desiderio di conferma sociale (da ottenere anche attraverso i social) e, talvolta, la scarsa consapevolezza degli adolescenti nel gestire la propria immagine online quando pubblicano sui loro profili social video e foto piuttosto intimi o sensuali, può aumentare il rischio di esporli ad un adescamento online. La Rete abbonda di contenuti inadeguati che offrono una rappresentazione distorta della sessualità e dei rapporti uomo-donna. La sessualità in Rete è spesso rappresentata in modo decontestualizzato e senza alcun richiamo alla dimensione affettiva ed emotiva dei soggetti.

La problematica dell'adescamento online (come quella del sexting), quindi, si inquadra in uno scenario più ampio di scarsa educazione emotiva, sessuale e di assenza di competenza digitale, in riferimento al modo in cui i/le ragazzi/e vivono la propria sessualità e la propria immagine online, al loro desiderio di esprimersi e affermare se stessi.

Fondamentale è portare avanti un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online.

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

Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video...).

Potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.

Per consigli e per un supporto è possibile rivolgersi alla Helpline di Generazioni Connesse (19696): operatori esperti e preparati sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che dei bambini, degli adolescenti, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti l'utilizzo dei nuovi media.

4.7 - Pedopornografia

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

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

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

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione **"Segnala contenuti illegali"** (Hotline).

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

Se si è a conoscenza di tale tipologia di reato è possibile far riferimento alla: Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Polizia di Stato – Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato – Commissariato online.

Studi in materia dimostrano come l'utilizzo di materiale pedopornografico possa essere propedeutico all'abuso sessuale agito ed è quindi fondamentale, in termini preventivi, intervenire per ridurre l'incidenza di tale possibilità.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022).

□ Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.

□ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti.

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).

□ Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.

□ Organizzare uno o più incontri informativi per la prevenzione dei rischi

associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.

□ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.

□ Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

□ Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire).

Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).

Nelle procedure:

- sono indicate le **figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso**.
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

Inoltre, la scuola **individua le figure che costituiranno un team**preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la **collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio** (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica.

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e

studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

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

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

- **Cyberbullismo**: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online**: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting**: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

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

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per

segnalare la presenza di materiale pedopornografico online.

Ogni qualvolta un componente della comunità scolastica abbia il sospetto o la certezza che uno/a studente/studentessa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online deve ricordare, innanzitutto, che nell'affrontare quanto accade non si è mai soli, bensì parte di una comunità all'interno e con il supporto della quale il problema va gestito.

5.2. - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero 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.

  Per tutti i dettagli fate riferimento agli allegati con le procedure.

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:

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;

- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

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

Il docente riveste la qualifica di pubblico ufficiale, 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; è quindi necessario sottolineare il dovere di sorveglianza ossia la "culpa in vigilando" attribuibile a chi è tenuto alla vigilanza dei minori.

Sarebbe opportuno prevedere momenti informativi, utilizzando anche la piattaforma Generazioni Connesse nella parte dei contenuti e dei materiali.

Per aiutare gli/le studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni sono stati previsti alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo mail specifico per le segnalazioni;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

5.3. - Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

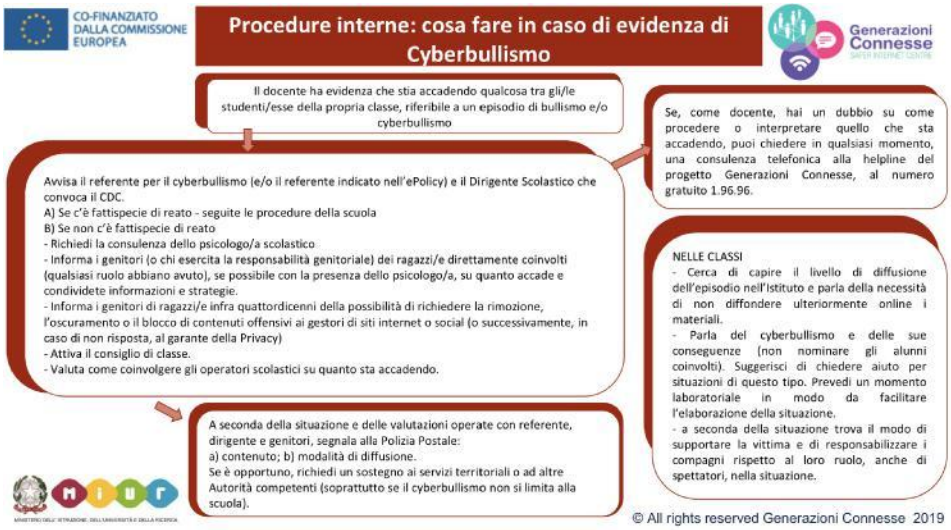
Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (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.

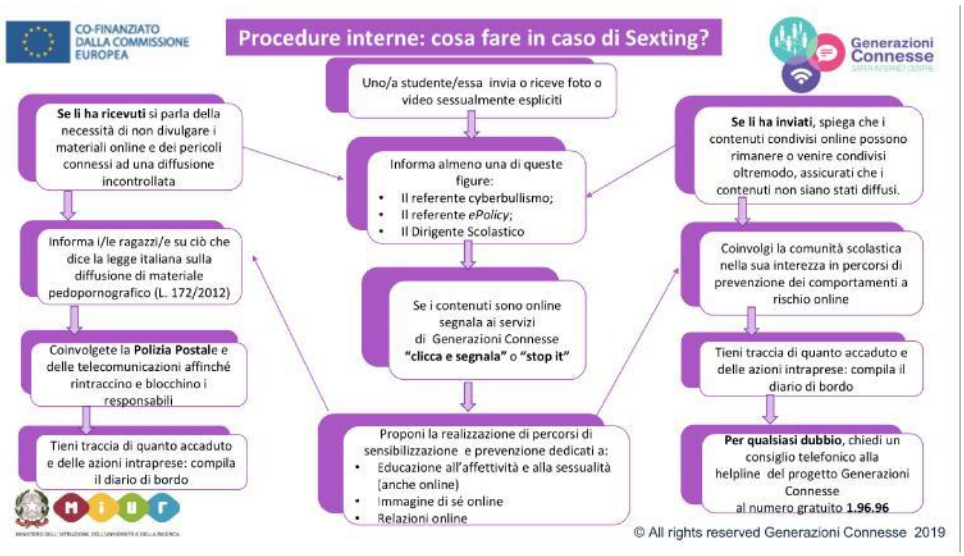
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare 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.

5.4. - Allegati con le procedure

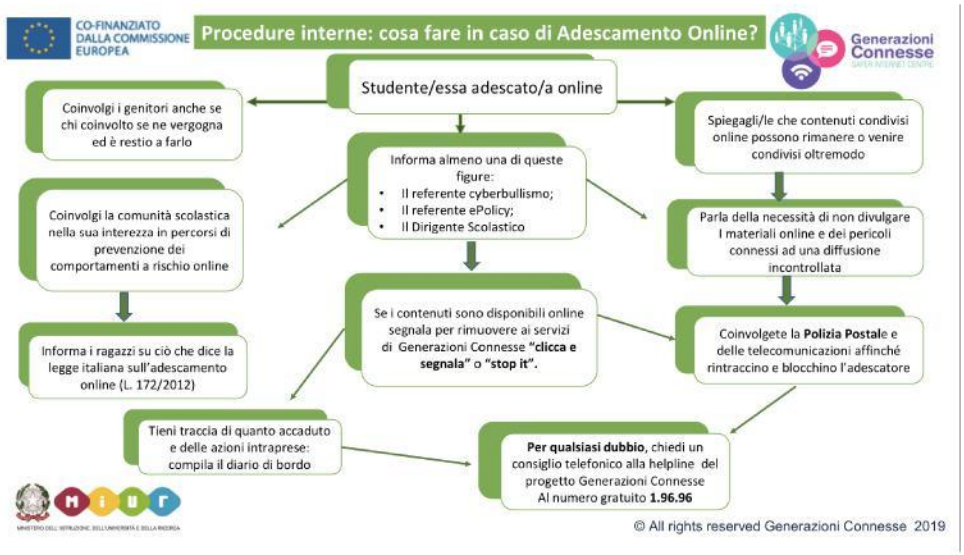
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



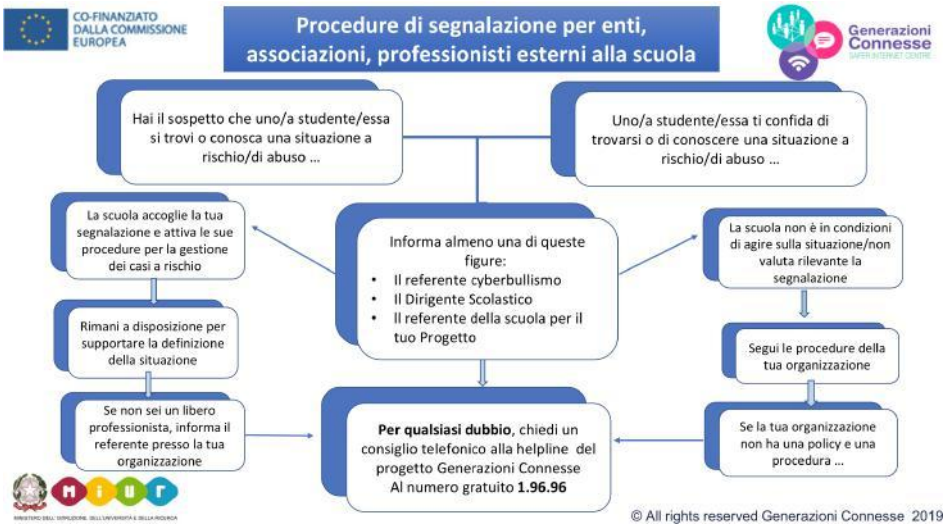
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola



Altri allegati

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

Il Liceo Visconti adotta le procedure e i moduli forniti dalla Piattaforma "Generazioni Connesse"

Il nostro piano d'azioni

Non è prevista nessuna azione.

IL DIRIGENTE SCOLASTICO
Prof.ssa Rita Pappalardo

Documento firmato digitalmente ai sensi del CAD e norme ad esso connesse