Documento di ePolicy

MIIC8DS00D

IC PRIMO LEVI/MILANO

VIA PISTOIA 30 - 20153 - MILANO - MILANO (MI)

Dirigente scolastica: Dott.ssa Chiara Bonetti

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

1. **Presentazione dell'ePolicy**
    1. Scopo dell'ePolicy
    2. Ruoli e responsabilità
    3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
    4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
    5. Gestione delle infrazioni alla ePolicy
    6. Integrazione dell'ePolicy con regolamenti esistenti
    7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
2. **Formazione e curricolo**
    1. Curricolo sulle competenze digitali per gli studenti
    2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
    3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
    4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
    1. Protezione dei dati personali
    2. Accesso ad Internet
    3. Strumenti di comunicazione online
    4. Strumentazione personale
4. **Rischi on line: conoscere, prevenire e rilevare**
    1. Sensibilizzazione e prevenzione
    2. Cyberbullismo: che cos'è e come prevenirlo
    3. Hate speech: che cos'è e come prevenirlo
    4. Dipendenza da Internet e gioco online
    5. Sexting
    6. Adescamento online
    7. Pedopornografia
5. **Segnalazione e gestione dei casi**
    1. Cosa segnalare
    2. Come segnalare: quali strumenti e a chi
    3. Gli attori sul territorio per intervenire
    4. Allegati con le procedure

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.

La Dirigente scolastica si impegna per garantire la sicurezza, anche online, di tutti i membri della comunità scolastica. È formata adeguatamente sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIM; promuove la cultura della sicurezza online e, insieme all’Animatrice Digitale e alle docenti referenti sulle tematiche del bullismo/cyberbullismo, propone corsi di formazione sull’utilizzo positivo e responsabile delle TIC. Inoltre, ha la responsabilità della gestione dei casi di gravi episodi di bullismo, cyberbullismo e uso improprio delle tecnologie digitali.

L’Animatrice digitale supporta il personale scolastico nell'uso delle tecnologie digitali e nell'integrazione della tecnologia nell'ambito educativo. Tra i compiti c'è la formazione interna del personale dell'Istituto sui temi legati alla scuola digitale o su esigenze specifiche della scuola. Per quanto concerne il supporto tenico-informatico, può aiutare il personale nell'utilizzo dei device. Può offrire consulenza sulle pratiche della sicurezza informatica e sulla gestione dei dati personali delle/degli alunne/i e del personale.

L'Amministratore della piattaforma Google Workspace e l'Amministratore del registro elettronico monitorano e rilevano eventuali episodi o problematiche connesse all’uso delle TIC a scuola, e hanno il compito di controllare che gli utenti autorizzati usino gli account forniti dall’Istituto e accedano alla Rete della scuola con apposita password solo per scopi istituzionali e consentiti (istruzione e formazione). Garantiscono, altresì, la tutela dei dati personali e il rispetto della privacy degli utenti.

Le Referenti del bullismo e cyberbullismo hanno il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, possono avvalersi della collaborazione delle Forze di Polizia, di associazioni, enti e centri di aggregazione giovanile del territorio.

Le/I Docenti hanno un ruolo centrale nel diffondere la cultura dell’uso responsabile

delle TIC e della Rete, promuovendo l'uso delle tecnologie digitali nella didattica. Le/I docenti hanno il dovere di accompagnare e supportare le/gli alunne/i nelle attività che prevedono l'uso di dispositivi tecnologici che si connettono alla Rete. Hanno il dovere morale e professionale di segnalare alla Dirigente scolastica qualunque problematica, violazione o abuso, anche online, che veda coinvolte/i le/i minori.

Il Personale Amministrativo, Tecnico e Ausiliario (ATA) può essere coinvolto nelle attività di formazione e autoformazione in tema di bullismo e cyberbullismo come anche nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

Le/Gli alunne/i si impegnano a utilizzare correttamente gli strumenti e le tecnologie digitali; con il supporto della scuola devono imparare a tutelarsi online, tutelare i propri compagni, partecipare attivamente a progetti e attività che riguardano l'uso positivo delle TIC e della Rete.

Ai Genitori è richiesto di essere partecipi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali anche in ambito extrascolastico. È importante che si relazionino in modo costruttivo con le/i docenti sulle linee educative che riguardano le TIC e la Rete, comunicando quando le/i proprie/propri figlie/figli non usano responsabilmente le tecnologie digitali o la rete messe a disposizione dalla scuola. Sottoscrivendo il Patto di Corresponsabilità, si impegnano ad accettare e condividere quanto scritto nell'E-Policy dell'Istituto.

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; devono, inoltre, promuovere la sicurezza online e l'adozione di comportamenti responsabili, assicurando anche la protezione e il rispetto della privacy delle/degli alunne/i durante le attività che si svolgono insieme, secondo le indicazioni standard definite nel paragrafo successivo (1.3).

Per un approfondimento sui ruoli e le responsabilità delle figure presenti a scuola: Legge 59/97, Art. 21 CO° 8; Legge N.165/2001 Art. 25; CCNL; DPR n. 275/99; Legge n.107/2015; Piano Nazionale Scuola Digitale.

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).

La scuola redige un'apposita informativa per le/i professioniste/i esterne/i che specifica ambiti di applicazione, codice di comportamento, procedure di segnalazione e provvedimenti nel caso di omessa segnalazione o violazione del codice di comportamento. Le figure professionali e le organizzazioni coinvolte in progetti, laboratori e attività devono prendere visione di tutti i documenti proposti dall'Istituto e sottoscriverli preliminarmente all'avvio dei programmi con le/gli alunne/i.

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.

L'E-Policy viene letta e condivisa con le/gli alunne/i nella versione standard e in una versione child friendly per la comunicazione e la sensibilizzazione sui temi in oggetto.

L'E-Policy viene anche menzionata nell'informativa relativa all'utilizzo dell'account Google Workspace della scuola.

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.

La scuola gestirà le infrazioni all'E-policy sulla base di quanto contenuto nel Regolamento d'Istituto.

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.

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.

Il gruppo di lavoro ePolicy monitorerà periodicamente l’aggiornamento dell’E-Policy.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare un evento volto a presentare il progetto Generazioni Connesse all'utenza scolastica.
- Organizzare almeno un incontro di lettura e condivisione dei temi dell’ePolicy con tutte le classi, per evidenziare la necessità di regolamentare azioni e comportamenti.
- Organizzare almeno un incontro di lettura e condivisione dei temi dell’ePolicy per i genitori dell’Istituto.

Azioni da svolgere nei prossimi 3 anni:

- Organizzare un evento volto a presentare il progetto Generazioni Connesse all'utenza scolastica.
- Organizzare almeno un incontro di lettura e condivisione dei temi dell’ePolicy con tutte le classi, per evidenziare la necessità di regolamentare azioni e comportamenti.
- Organizzare almeno un incontro di lettura e condivisione dei temi dell’ePolicy per i genitori dell’Istituto.

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.

Avendo come riferimento le aree di competenza individuate dal DigComp 2.2, si intendono sviluppare le competenze delle 5 aree:

Area 1: "Alfabetizzazione su informazioni e dati" 1.1 Navigare, ricercare e filtrare dati, informazioni e contenuti digitali 1.2. Valutare dati, informazioni e contenuti digitali 1.3. Gestire dati, informazioni e contenuti digitali.

Area 2: "Comunicazione e collaborazione" 2.1. Interagire con gli altri attraverso le tecnologie 2.2. Condividere informazioni attraverso le tecnologie digitali 2.3. Esercitare la cittadinanza attraverso le tecnologie digitali 2.4. Collaborare attraverso le tecnologie digitali 2.5. Netiquette 2.6. Gestire l'identità digitale.

Area 3: "Creazione di contenuti digitali" 3.1. Sviluppare contenuti digitali 3.2. Integrare e rielaborare contenuti digitali 3.3. Copyright e licenze 3.4. Programmazione.

Area 4: “Sicurezza” 4.1. Proteggere i dispositivi 4.2. Proteggere i dati personali e la privacy 4.3. Proteggere la salute e il benessere 4.4. Proteggere l’ambiente.

Area 5: "Risolvere problemi".5.1. Risolvere problemi tecnici 5.2. Individuare bisogni e risposte tecnologiche 5.3. Utilizzare in modo creativo le tecnologie digitali 5.4. Individuare i divari di competenze digitali.

I TRAGUARDI PER LO SVILUPPO DELLE COMPETENZE

Al termine della Scuola primaria:

- Padroneggiare le tecnologie in contesti comunicativi concreti.
- Esercitare un uso consapevole dei materiali e delle fonti documentali digitali disponibili sul web.
- Conoscere rischi e pericoli nella ricerca e nell’impiego delle fonti.
- Rispettare la netiquette.

Al termine della Scuola secondaria di primo grado:

- Essere in grado di avvalersi consapevolmente e responsabilmente dei mezzi di comunicazione virtuali.
- Essere consapevole dei rischi della rete e come riuscire a individuarli.
- Saper gestire le emozioni che possono emergere all’interno del contesto virtuale in cui si muove (Social Network, gioco on line, chat).
- Conoscere le regole essenziali della Netiquette (bon ton in rete).
- Conoscere i rischi della rete.
- Conoscere e gestire le dipendenze dai social network.

I traguardi saranno inseriti nel curricolo verticale di Istituto.

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.

L'Istituto incoraggia la partecipazione del personale docente a iniziative promosse sia direttamente dalla scuola (ad es. con l'ausilio dell'Animatrice digitale), dalle reti di scuole e dall'amministrazione, sia quelle liberamente scelte dalle/dai docenti (anche online) sulle TIC e si impegna a organizzare momenti di formazione sui metodi e sugli strumenti della didattica digitale.

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.

I momenti di formazione e aggiornamento verranno realizzati a partire dall'analisi del fabbisogno formativo e conoscitivo del personale docente sull'utilizzo e l'integrazione delle TIC nella didattica e di altri significativi argomenti rilevati attraverso gli incontri collegiali.

Sarà incoraggiata la partecipazione delle/dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto "Generazioni Connesse" e l'organizzazione di incontri con professionisti della scuola o con esperti esterni, enti/associazioni.

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.

L'Istituto promuove momenti di formazione e sensibilizzazione sulle tematiche in oggetto attraverso incontri online con enti e associazioni (ad es. Fare X Bene) e con le Forze dell'Ordine.

Momenti formativi di approfondimento (progetti specifici, laboratori, eventi, giornate, etc…) con genitori e alunne/i saranno utili per sensibilizzare l'intera comunità educante su un corretto uso delle tecnologie digitali e sulle potenzialità della rete in ambito scolastico ed extrascolastico.

Il nostro piano d'azioni

AZIONI

Scegliere almeno 1 di queste azioni

- Organizzare e promuovere per il corpo docente incontri 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.
- Organizzare incontri con esperti per l'utenza scolastica sulle competenze digitali e sull'educazione alla cittadinanza digitale.

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

Scegliere almeno 1 di queste azioni

- Organizzare e promuovere per il corpo docente incontri 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.
- Organizzare incontri con esperti per l'utenza scolastica sulle competenze digitali e sull’educazione alla cittadinanza digitale.

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 documentazione relativa alla privacy è contenuta all'interno del sito web di Istituto.

La scuola, nel suo fondamentale compito di tutela dellla privacy delle/degli alunne/i e delle loro famiglie, si pone l'obiettivo di informare e soprattutto rendere consapevoli le/gli alunne/i di quanto sia importante tutelare il diritto alla riservatezza di sé stessi e degli altri. In fase di iscrizione delle/degli alunne/i alla scuola i genitori sottoscrivono un'informativa sul trattamento dei dati personali in ottemperanza all'art. 13 D.Lgs 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).

All'inizio del ciclo di istruzione i genitori rilasciano il consenso all'utilizzo di materiale fotografico e audiovisivo e degli elaborati delle/degli alunne/i per pubblicarli sul sito dell'Istituto. In caso di utilizzo di piattaforme digitali condivise, viene condivisa l'informativa sul trattamento dei dati. In caso di attività di ampliamento dell'offerta formativa, organizzate in collaborazione con Enti esterni, viene richiesto preventivamente ai genitori il consenso informato alle riprese audio/ video e al loro eventuale utilizzo per scopi didattici, informativi e divulgativi anche tramite pubblicazione su siti web. L'accesso ai dati riportati nel registro elettronico (ritardi, assenze, note e valutazioni) è riservato ai genitori della scuola primaria e secondaria di primo grado tramite l'invio di una password di accesso strettamente personale.

Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc.

Le scuole hanno l'obbligo quindi di informare (tramite apposita informativa) gli interessati (alunne/i, genitori, personale della scuola) delle caratteristiche e modalità del trattamento dei loro dati, indicando i responsabili dello stesso. È importante, inoltre, che le scuole verifichino i loro trattamenti, controllando se i dati siano eccedenti rispetto alle finalità perseguite, in accordo con quanto suggerito dal Garante per la protezione dei dati personali, il quale stabilisce che "le scuole devono rendere noto alle famiglie e ai ragazzi, attraverso un'adeguata informativa, quali dati raccolgono e come li utilizzano". Genitori e alunne/i, pertanto, hanno il diritto di conoscere quali informazioni sono trattate dall'Istituto scolastico, farle rettificare se inesatte, incomplete o non aggiornate.

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.

L'Istituto valuta tutti gli aspetti legati alla sicurezza nel momento in cui permette ad alunne/i e docenti l’accesso alla rete tramite i dispositivi della scuola e la rete scolastica. In riferimento alla security, non è sufficiente prestare attenzione all’infrastruttura hardware e alla rete, ma è necessario considerare anche la sicurezza di tutti gli aspetti che riguardano la gestione degli account degli utenti (in modo differenziato tra alunne/i, genitori rappresentanti di classe e genitori membri del Consiglio di Istituto, insegnanti e personale ATA), il filtraggio dei contenuti e gli

aspetti legali in relazione prevalentemente alla privacy.

L’accesso a internet è possibile per la didattica in tutte le aule e negli spazi multimediali.Per tutto il personale della scuola la connessione alla rete wi-fi è accessibile tramite una password. Le postazioni presenti in segreteria sono accessibili solo dal personale amministrativo con utenza e password e una rete dedicate.

L'Istituto condivide una netiquette sul corretto utilizzo dei device e della rete contenuta all'interno dell'informativa.

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.

Fra gli strumenti di comunicazione esterna si fa menzione del sito web di Istituto. Fra quelli di comunicazione interna, invece, il registro elettronico Argo e la piattaforma Google Workspace for Education.

In riferimento all’uso degli strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne,è importante ricordare quello che si può definire “diritto alla disconnessione” (art. 22 - Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola del CCNL 2016/2018).

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.

L'E-Policy sarà oggetto di aggiornamento nella fase di revisione del Regolamento di Istituto in materia di utilizzo dei dispositivi personali per uso didattico.

Il nostro piano d'azioni

AZIONI

- Organizzare uno o più eventi o attività volti a formare l'utenza dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare l'utenza dell'Istituto sui temi dell'accesso a 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 formare l'utenza dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare l'utenza dell'Istituto sui temi dell'accesso a 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.*

Il nostro Istituto, impegnato sui temi della sensibilizzazione e prevenzione, offre alle/agli alunne/i percorsi in grado di informarle/i e formarle/i sul corretto e sicuro utilizzo delle nuove tecnologie, rendendo anche disponibile all'utenza uno sportello di ascolto.

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).

Un'indicazione operativa da considerare per un efficace intervento è rendersi conto se l'azione oggetto di analisi sia effettivamente cyberbullismo o sia riconducibile ad altra tipologia di comportamenti scorretti. Altri elementi utili ad effettuare tale valutazione

sono le modalità in cui avvengono (alla presenza di un "pubblico"? Tra coetanei?) e l'età dei protagonisti.

Un'altra indicazione operativa è la valutazione di uno stato di disagio vissuto dalla/dal minore, per cui potrebbe essere necessario rivolgersi a un servizio di supporto psicologico e/o di mediazione. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza.

Per quanto riguarda la necessità di segnalazione e rimozione, ciascuna/ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità della/del minore) che sia stata/o 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'interessata/o può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Nel caso in cui ci si trovi di fronte a un possibile reato, si potrà fare riferimento agli uffici preposti delle Forze di Polizia per permettere alle autorità competenti l'approfondimento della situazione. Alcuni atti di bullismo possono configurarsi come reati, ad es. percosse (art. 581), lesione personale (art. 582), ingiuria (art. 594), diffamazione (art. 595), violenza privata (art. 610), minaccia (art. 612), danneggiamento (art. 635). Nei casi più gravi, basta la denuncia a un organo di polizia o all'autorità giudiziaria per attivare un procedimento penale (per es. lesioni gravi, minaccia grave, molestie); negli altri casi, la denuncia deve contenere la richiesta che si proceda penalmente contro l'autore di reato (querela).

Come forma di supporto, è possibile rivolgersi alla Helpline di Telefono Azzurro per Generazioni Connesse: gli operatori sono sempre a disposizione del personale scolastico, delle/degli alunne/i e dei genitori e/o adulti che a vario titolo necessitano di un confronto e di un aiuto.

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.

In relazione al fenomeno, il nostro Istituto si propone di attivare percorsi didattici con i seguenti obiettivi:

1. Incoraggiare le/gli alunne/i a riflettere sul linguaggio come strumento per negare o sostenere i diritti degli altri.

2. Aiutare le/gli alunne/i a riconoscere gli stereotipi su cui spesso si fondano forme di hate speech (pregiudizi legati alla razza, al genere, all’orientamento sessuale).

3. Promuovere tra le/gli alunne/i la solidarietà, il rispetto, l'empatia.

4.Promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network.

5. Stimolare nelle/negli alunne/i il pensiero critico.

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?

La scuola supporta le/gli alunne/i nel riconoscere le potenzialità del digitale ma anche i rischi connessi a un abuso della tecnologia.

Le/I docenti sensibilizzano le/gli alunne/i su concetti quali la gestione del tempo trascorso su social o su Internet, la comunicazione online (es. comprensione delle dinamiche di relazione online, dei concetti di "identità digitale" e di "netiquette"), la ricerca e gestione delle informazioni (es. riconoscere le fake news, attraverso una ricerca delle fonti), la creazione di contenuti digitali (con particolare attenzione al contenuto e a problemi quali il diritto di privacy, il diritto d'autore etc.), la ludopatia (dipendenza dai giochi, con problemi connessi quali, ad es., l'adescamento 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.

A livello preventivo, il nostro Istituto attiva percorsi di informazione/formazione destinati all'utenza scolastica, nel rispetto dell'età e della sensibilità di ciascuna/o, per approfondire i rischi e le conseguenze di episodi di sexting.

I contenuti sessualmente espliciti possono diventare materiale di ricatto assumendo la forma di "revenge porn", letteralmente "vendetta porno", fenomeno che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte (la Legge 19 luglio 2019 n. 69, all'articolo 10 ha introdotto in Italia il reato di revenge porn, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti).

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.

Il miglior modo per prevenire casi di adescamento online è accompagnare le/gli alunne/i in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Questi percorsi hanno la funzione di renderle/i emotivament più sicure/i e pronte/i ad affrontare eventuali situazioni a rischio, imparando a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri.

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.

Il nostro piano d'azioni

AZIONI

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse

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.

- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

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.

Tra i principali problemi che si possono presentare nell'uso di Internet online ricordiamo:

- esposizione a contenuti violenti e/o non adatti all'età;

- videogiochi diseducativi;

- pubblicità ingannevoli;

- fake news;

- possibili contatti con adulti che vogliono conoscere e avvicinare bambine/i o ragazze/i (adescamento);

- rischio di molestie o maltrattamenti da coetanei (cyber-bullismo); -

- scambio di materiale a sfondo sessuale (sexting);

- uso eccessivo di Internet/cellulare (dipendenza)

Le/I docenti dell'Istituto si propongono di riflettere insieme con le/gli alunne/i su questi rischi. Il monitoraggio costante delle relazioni interne alla classe è fondamentale per individuare possibili situazioni di disagio e intervenire tempestivamente, anche mediante il ricorso alle figure specializzate, per sostenere l'alunna/o nelle situazioni di difficoltà personale e indirizzare il gruppo verso l'instaurazione di un clima positivo. Tale percorso interno potrà essere ulteriormente rinforzato dalla partecipazione a progetti e/o iniziative legate a queste tematiche, cui il nostro istituto ha già dato particolare attenzione e continuerà a farlo nell'intento di collaborare con Enti e/o Associazioni di comprovata affidabilità nel percorso di affiancamento e supporto delle/degli alunne/i.

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.

La segnalazione del caso può essere effettuata da qualsiasi docente, dai genitori/tutori e dalle/dagli alunne/i tramite la comunicazione alla/al docente Coordinatrice/Coordinatore della classe. Quest'ultima/o comunicherà subito a mezzo e-mail alla Dirigente scolastica le informazioni ricevute. Sarà la Dirigente scolastica, sentito anche il parere delle Referenti del bullismo/cyberbullismo, a valutare se la segnalazione debba essere rivolta ad organi esterni alla scuola, quali la Polizia Postale o i Servizi Sociali, o se il caso vada gestito all'interno della scuola con il coinvolgimento del Consiglio di Classe e delle famiglie delle/degli alunne/i coinvolte/i. La tipologia di intervento sarà determinata grazie anche alla valutazione approfondita che verrà svolta dalle docenti referenti del bullismo/cyberbullismo in accordo con il Consiglio/Team di classe, raccogliendo tutte le informazioni possibili, anche attraverso colloqui di approfondimento con gli attori coinvolti. L'ultima fase della procedura è il monitoraggio per supervisionare la gestione del caso e valutare l'efficacia

dell'intervento sia a breve che a lungo termine.

Docenti referenti per la prevenzione e il contrasto di atti di bullismo e cyberbullismo: Angela Ragozzino; Lucia Taddeo.

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.

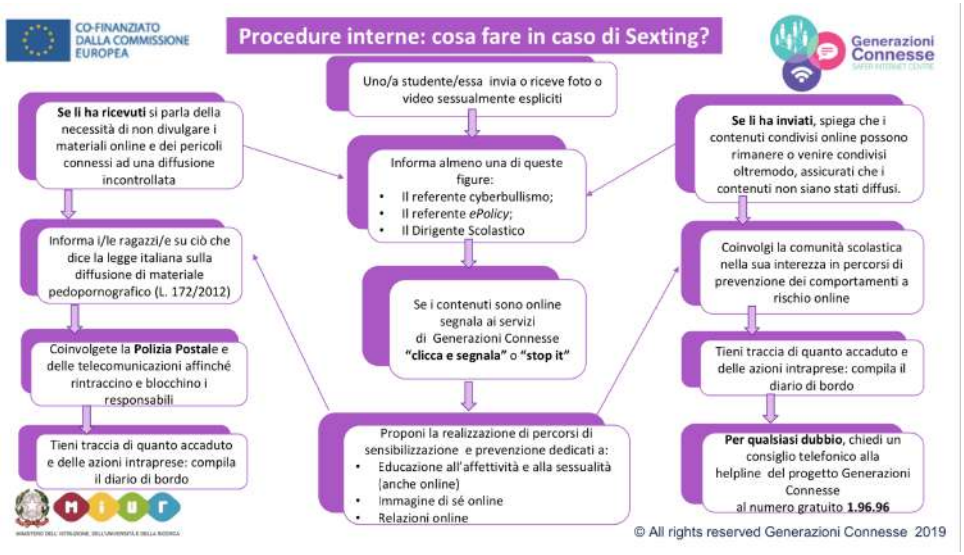
5.4. - Allegati con le procedure

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

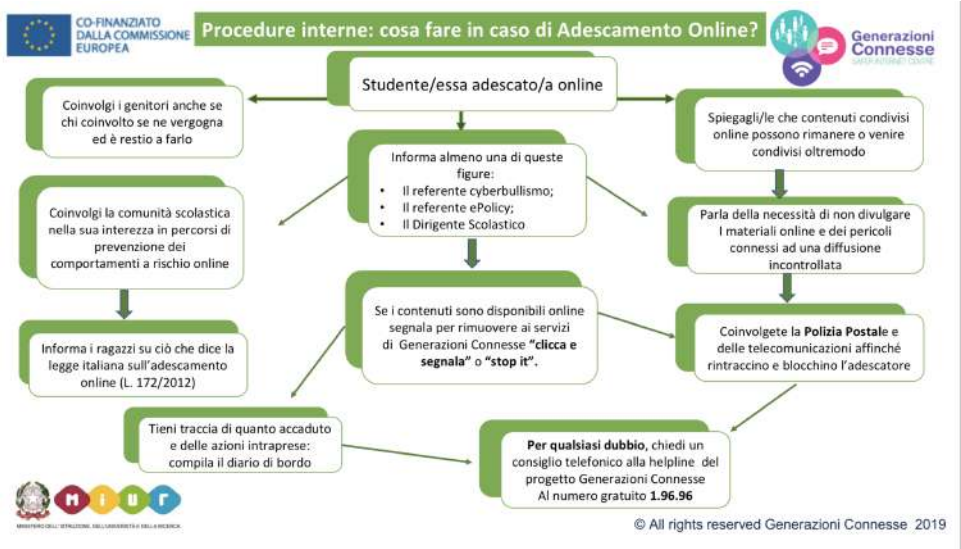




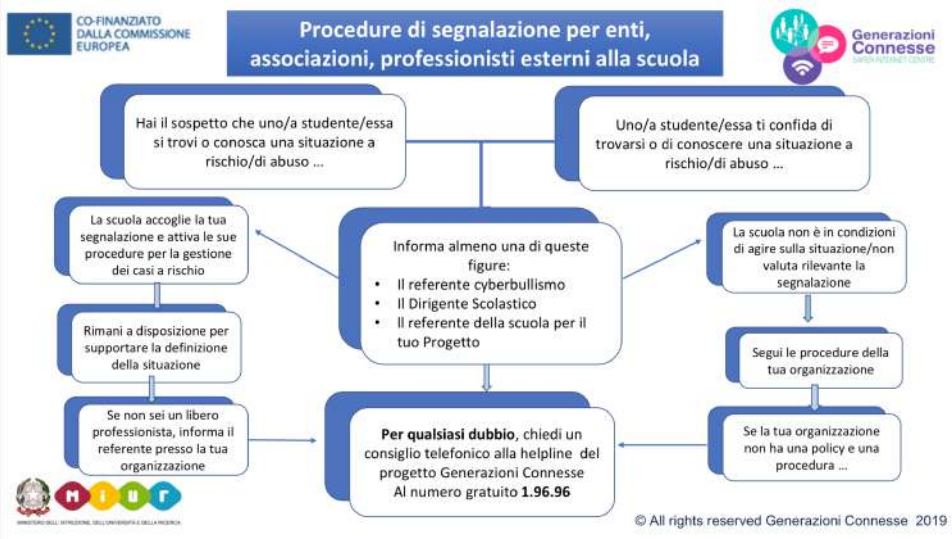
Procedure interne: cosa fare in caso di sexting?



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 nostro piano d'azioni

Sulla base delle "Linee guida per l'uso positivo delle tecnologie digitali e della prevenzione dei rischi nelle scuole", l'Istituto intende promuovere una collaborazione sinergica e incoraggiare l'alleanza educativa tra scuola-famiglia-servizi territoriali,

Con la promozione dell'Educazione Civica Digitale, sarà valorizzato il coinvolgimento di tutti gli attori della scuola, alunne/i, docenti, genitori e personale ATA, per affermare un modello di scuola come comunità.

L'azione di sensibilizzazione sui temi del progetto, già intrapresa dall'Istituto, proseguirà con interventi educativi ed azioni di supporto e prevenzione di comportamenti a rischio, anche con la collaborazione di associazioni ed enti del territorio, per la promozione dell'educazione al rispetto e alla responsabilità e lo sviluppo del pensiero critico.