Documento di ePolicy

PAIC8AD00Q

I.C. LOMBARDO RADICE -PA

C.SO CALATAFIMI 241/A - 90129 - PALERMO - PALERMO (PA)

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.

Lo scopo di questo documento è quello di raccogliere e illustrare le linee guida per la prevenzione e il contrasto del bullismo e cyberbullismo nel nostro Istituto, in conformità con le linee di

orientamento del MIUR.

Inoltre il documento ha lo scopo di fornire ai docenti uno strumento di lavoro che possa aiutarli ad affrontare le sempre nuove sfide educative che potrebbero presentarsi, dato l'uso e l'evolversi costante delle nuove tecnologie.

Si ritiene, pertanto, necessario avviare una politica di sicurezza della navigazione on line, volta ad un controllo dell'uso delle strumentazioni digitali e alla diffusione di buone pratiche di comunicazione anche sui social network.

Il nostro lavoro è stato realizzato tenendo conto delle indicazioni proposte dal progetto: "www.generazioniconnesse.it" realizzato su indicazioni del MIUR

Riferimenti normativi

Il bullismo e il cyberbullismo devono essere conosciuti e combattuti così come previsto:

• dall' art. 3 della Costituzione italiana (Principio di uguaglianza);

•dall'art. 34 della Costituzione italiana (diritto allo studio);

• dalla Direttiva Ministeriale n.16 del 5 febbraio 2007 recante "Linee di indirizzo generali ed azioni a livello nazionale per la prevenzione e la lotta al bullismo";

• dalla direttiva Ministeriale n. 30 del 15 marzo 2007 recante "Linee di indirizzo ed indicazioni in materia di utilizzo di 'telefoni cellulari' e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, dovere di vigilanza e di corresponsabilità dei genitori e dei docenti";

• dalla direttiva Ministeriale n. 104 del 30 novembre 2007 recante "Linee di indirizzo e chiarimenti interpretativi ed applicativi in ordine alla normativa vigente posta a tutela della privacy con particolare riferimento all'utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire e/o divulgare immagini, filmati o registrazioni vocali";

• dal D.P.R. 249/98 e 235/2007 recante"Statuto delle studentesse e degli studenti";

• dalle Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo, MIUR aprile 2015;

• dagli art. 581 (percosse) - 582 (lesione personale) - 595 (diffamazione) - 610 (violenza privata) - 612 (minaccia)- 635 (danneggiamento) del Codice Penale;

• dagli art. 2043 (risarcimento per fatto illecito) - 2047 (danno cagionato dall'incapace) – 2048 (responsabilità dei genitori, dei tutori, dei precettori e dei maestri d'arte) del Codice Civile.

• dalle Linee di orientamento per la prevenzione e il contrasto del cyberbullismo, MIUR ottobre 2017;

• dalla Legge del 29 maggio 2017 n.71 (disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo).

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.

Ruoli e responsabilità

Il Dirigente Scolastico: (prof. F.sco Paolo Camillo) responsabile per la sicurezza dei dati e garante dell'applicazione della E-Policy, coinvolge nella prevenzione e contrasto al fenomeno del bullismo e del cyberbullismo tutta la comunità scolastica, promuove la discussione all'interno della scuola, attraverso gli organi collegiali, favorendo la condivisione di regole di comportamento comuni per il contrasto e la prevenzione dei fenomeni del bullismo e del cyberbullismo.

Il Referente bullismo e Cyberbullismo: (prof.ssa Maria Cubito) promuove attività, incontri, eventi funzionali alla prevenzione delle problematiche inerenti al bullismo e al cyberbullismo.

Animatore Digitale: (ins. Caterina Ferrera) promuove la diffusione dei contenuti della E-Policy e organizza attività volte all'uso sicuro e consapevole del web.

Direttore dei Servizi Generali e Amministrativi:
(Dott. Provvidenza Di Girolamo)
assicura l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio; garantisce il funzionamento dei diversi canali di comunicazione della scuola (circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni; notifica documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.

Docenti, Personale ATA, genitori ed alunni: sono tenuti a conoscere e mettere in pratica i regolamenti redatti dall'Istituto e a segnalare tempestivamente eventuali violazioni. I docenti sono invitati a partecipare alle attività di formazione proposte dai referenti.

Condivisione e comunicazione della Policy all'intera comunità scolastica

La E- Policy viene pubblicata sulla Home Page del sito della scuola dopo essere stata approvata dal Collegio dei Docenti.

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).

Le associazioni o le organizzazioni extrascolastiche, gli esperti esterni che potrebbero essere chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sia per breve tempo, sia per progetti che prevedano maggiore tempo, dovranno prendere atto di quanto stilato nell' E-policy dell'Istituto o eventualmente sottoscrivere un'informativa sintetica del documento in questione, nel rispetto della privacy e della tutela dei minori e della loro immagine.

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.

Condivisione e comunicazione della ePolicy all'intera comunità scolastica

La presente epolicy è stata redatta dalla commissione bullismo/cyberbullismo, un gruppo di lavoro costituito nell'a.s. 2019/2020 e condivisa dall'animatore digitale.

Condivisione e comunicazione della ePolicy al personale scolastico

Le norme adottate dalla scuola in materia di sicurezza nell'utilizzo del digitale saranno rese note tramite pubblicazione del presente documento sul sito web della scuola.

Condivisione e comunicazione della ePolicy ai genitori

Le famiglie saranno informate in merito alla linea di condotta adottata dalla scuola per un uso sicuro e responsabile delle tecnologie digitali e di internet attraverso la condivisione del presente documento sul sito web della scuola.

Condivisione e comunicazione della ePolicy agli alunni

Attraverso la condivisione del patto educativo di corresponsabilità, attività in classe che portino a riflettere su rischi e opportunità del web.

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.

Gestione delle infrazioni alla Policy

La violazione delle norme, previste dal regolamento, comporta l'eventuale irrogazione di sanzioni disciplinari, secondo quanto previsto dal Regolamento di disciplina e dal Patto di Corresponsabilità controfirmato da scuola e genitori. Nei casi più gravi potrebbero anche configurarsi reati perseguibili d'ufficio o a querela di parte, come previsto dai riferimenti normativi. Si rinvia al Regolamento d'Istituto e al Patto di Corresponsabilità.

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.

La Policy è coerente con quanto stabilito nel regolamento di Istituto.

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 presente documento potrà essere aggiornato, implementato e migliorato annualmente.

Il nostro piano d'azioni

Azione da svolgere entro un'annualità scolastica:

.

- Organizzare un evento di presentazione e conoscenza dell'ePolicy rivolto a

studenti e docenti

Azioni da svolgere nei prossimi 3 anni:

- Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto ai genitori

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.

Alla fine della scuola primaria e al termine del primo ciclo di istruzione le competenze digitali vengono certificate sulla base dei seguenti profili.
• **Primaria**:l'alunno sa usare le tecnologie in contesti comunicativi concreti per ricercare dati e informazioni e per interagire con soggetti diversi.
• **Secondaria di primo grado**: l'alunno sa usare con consapevolezza le tecnologie per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento (fake news), di controllo e di verifica e per interagire con soggetti diversi.

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 competenze digitali, nel nostro istituto vengono promosse in maniera trasversale dai docenti, sulla base delle loro pratiche di insegnamento. Dal corrente a. s. è stato redatto un apposito regolamento per la **Didattica digitale integrata.**
Il percorso di formazione specifica dei docenti sull'utilizzo delle TIC non può ritenersi mai concluso, ma deve essere "permanente" in relazione all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono in maniera costante ed autonoma i ragazzi. Può prevedere momenti di autoaggiornamento e di formazione personale o collettiva, anche attraverso i percorsi webinar su www.generazioniconnesse.it

---

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'Animatore Digitale, insieme al team che redige il presente documento, avrà il compito di promuovere la didattica multimediale, anche attraverso l'organizzazione di incontri e webinar con esperti in modalità online, per formare il corpo docente sulle modalità di gestione dei rischi derivanti dal non corretto uso delle teconologie digitali.
Con la partecipazione dell'Istituto al progetto "Generazioni Connesse" del Safer Internet Center, si prevede anche una fase di autoaggiornamento degli insegnanti tramite materiali informativi sulla sicurezza in internet reperibili sul web, in particolare sul sito di Generazioni Connesse (www.generazioniconnesse.it).

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.

La ePolicy integrerà il Patto di Corresponsabilità Educativa sottoscritto dai genitori e verrà condivisa con gli alunni.
Verranno forniti ai genitori materiali on line, reperibili sulla piattaforma www.generazioniconnesse.it, indicanti i rischi che i minori possono correre nell'uso non corretto della rete e dei social network.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco di una annualità)

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.

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

- 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 incontri 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.

Durante la fase di iscrizione degli alunni alla scuola, i genitori sottoscrivono un'informativa sul trattamento dei dati personali in ottemperanza all'art. 13 D.Lgs 30 giugno 2013 , n. 196.
All'inizio dell'anno scolastico i genitori rilasciano il consenso all'utilizzo di materiale fotografico e audiovisivo riservato ed elaborati degli alunni per esporli anche in sedi diverse da quelle dell'Istituto, quali pubblicazioni in formato digitale e siti WEB.
In caso di utilizzo di piattaforme digitali condivise o di strumenti per la creazione e la gestione di classi virtuali, viene acquisito preventivamente il consenso informato dei genitori. 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. Responsabile della protezione dei dati designato ai sensi dell'art. 37 del Regolamento UE è il dott. Badami Mario.

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.

La scuola è dotata di connessione internet, fibra ottica, rete wi-fi.

In tutto, nel nostro Istituto sono presenti 20 LIM e due laboratori informatici. Gli edifici sono cablati. I laboratori di informatica sono regolamentati dalle seguenti norme:

1. Le apparecchiature presenti nella scuola sono un patrimonio comune, quindi, vanno usate con il massimo rispetto.
2. Quando un insegnante, con la classe, usufruisce del laboratorio deve registrare il proprio nome e la classe nell’apposito registro delle presenze di laboratorio, indicando l’orario di ingresso, quello di uscita.
3. L’ingresso degli allievi nei laboratori è consentito solo in presenza dell’insegnante.
4. Il docente accompagnatore è responsabile del corretto uso didattico delle apparecchiature.
5. Nei laboratori è vietato utilizzare CD personali o pendrive se non dopo opportuno controllo con sistema di antivirus aggiornato.
6. All’uscita dal laboratorio sarà cura di chi lo ha utilizzato spegnere le strumentazioni in modo corretto.
7. In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile del laboratorio, che provvederà alla risoluzione del problema.
8. I software installati sono ad esclusivo uso didattico.

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.

L’account di posta elettronica è quello istituzionale, utilizzato dagli uffici amministrativi, sia per la posta in ingresso che in uscita. Le credenziali sono in possesso del personale amministrativo.

Il sito istituzionale della scuola http://www.icslombardoradice.edu.it/è attivo e gestito da un responsabile nominato dal dirigente.

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.

Per gli studenti: è vietato l'utilizzo di cellulari per l'intera durata delle attività scolastiche (compreso l'intervallo). Gli alunni con Bisogni Educativi Speciali potranno utilizzare il proprio notebook o tablet e la connessione wifi della scuola. E'consentito a tutti gli alunni in casi specifici concordati con il docente (uso di e-book, produzioni multimediali) l'utilizzo di dispostivi elettronici personali per scopi didattici.
Per i docenti: durante il loro orario di servizio è consentito l'utilizzo di dispostivi elettronici personali solo ed esclusivamente per fini didattici.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco di una annualità).

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti

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

- 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

- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto 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.*

Attraverso il sito della scuola, saranno pubblicizzati i materiali a disposizione delle famiglie (tratti dal sito www.generazioniconnesse.it) per metterle al corrente dei problemi legati ad un uso non corretto di internet e delle tecnologie digitali, anche al di fuori della scuola.
Data l'enorme diffusione delle tecnologie digitali e la possibilità di accesso a Internet da parte dei più giovani, si sono registrati profondi cambiamenti nelle dinamiche relazionali e in quelle identitarie, e sono cambiati linguaggi, modalità di comunicazione, abitudini e stili di vita. Quindi, se, da una parte, le Tecnologie dell'Informazione e della Comunicazione (TIC) sono parte integrante della vita quotidiana dei più giovani, in quanto strumenti privilegiati di comunicazione e di relazione, di informazione, di studio, di creatività e partecipazione, dall'altra parte, esse ci costringono a porre però delle questioni associate alla "sicurezza" e al comportamento sociale. Ci si trova di fronte ad

una realtà complessa, pensata prevalentemente per un mondo adulto e nella quale trovano spazio contenuti e comportamenti potenzialmente dannosi, fruiti, ormai, però da sempre più esperti bambini ed adolescenti.
I rischi online rappresentano tutte quelle situazioni problematiche derivanti da un uso non consapevole e non responsabile delle tecnologie digitali da parte di bambini/e, ragazzi e ragazze.
E' fondamentale prevenire e sapere riconoscere tali rischi, per riuscire a contenerli e incanalarne le potenzialità verso un uso consapevole.

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).

Come riportato nell'integrazione sul bullismo e sul cyberbullismo del Regolamento d'Istituto, sono da considerarsi tipologie persecutorie qualificate
come Bullismo:
- la sopraffazione fisica, verbale e/o psicologica
- la violenza fisica, psicologica o l'intimidazione del gruppo, specie se reiterata;
- l'intenzione di nuocere;
- l'isolamento sociale della vittima
Rientrano nel Cyberbullismo:
- **FLAMING**: litigi nei forum di discussione o sui social, con l'uso di un linguaggio violento e volgare.
- **HARASSMENT:** molestie attuate attraverso l'invio ripetuto di messaggi offensivi
- **CYBERSTALKING**: invio ripetuto di messaggi che includono esplicite, minacce fisiche.
- **DENIGRAZIONE**: sparlare, attraverso messaggi, di qualcuno per danneggiare gratuitamente e con cattiveria la sua reputazione.
- **OUTING ESTORTO:** registrazione di confidenze per poi inserirle integralmente in un blog pubblico.
- **TRICKERY**: spinta, attraverso l'inganno, a rivelare informazioni imbarazzanti e riservate per renderle poi pubbliche in rete.
- **IMPERSONATION**: appropriazione dell'account di un'altra persona.
- **ESCLUSIONE**: estromissione intenzionale di una persona da un gruppo online.
- **HAPPY SLAPPING:** ripresa, con il telefono, (o macchina fotografica o videocamera), di scene violente al fine di mostrarle ad amici o di diffonderle sulla rete.
- **EXPOSURE**: pubblicare informazioni private e/o imbarazzanti su un'altra persona.
- **SEXTING:** invio di messaggi via smartphone ed Internet, corredati da immagini a sfondo sessuale.

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.

Il nostro Istituto intende, anche grazie all'introduzione dell'insegnamento trasversale della ed. civica, imprimere una forte impronta nella direzione di fornire adeguati strumenti ai docenti e agli alunni che portino ad un radicale cambiamento di rotta, rispetto al fenomeno dell'hate speech. Ciò potrà essere raggiunto con percorsi e attività mirati che privilegino:

- l'educazione interculturale e il coinvolgimento attivo dei ragazzi e delle ragazze.

- l'educazione all'affettività e alla gestione della rabbia, attraverso percorsi che tengano conto della delicata fase di passaggio dall'adolescenza all'età adulta, senza mai porsi in posizione guidicante, in un continuo percorso di apprendimento permanente "laboratoriale".

- media education.

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?

Si ritiene necessario fornire informazioni sulla dipendenza patologica da gaming on line e sul fatto che ciò può rappresentare una vera e propria patologia, che compromette la salute e le relazioni sociali e che in taluni casi può rappresentare un vero e proprio illecito. Il nostro Istituto è interessato a promuovere, nei prossimi anni, dei percorsi sul cosiddetto "benessere digitale", al fine di concentrarsi in particolare sulla comprensione delle dinamiche di relazione online e sui concetti di "identità digitale" e di "netiquette" (una sorta di galateo che dovrebbe ispirare i nostri

comportamenti digitali alla tutela del proprio e dell'altrui benessere psicologico e alla cura della relazione).

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.

Durante le lezioni si affronterà, con le classi della scuola superiore di primo grado, il delicato argomento, attraverso la visione di video informativi. Dal momento che internet, come ogni potente strumento, nasconde moltissime insidie si cercheranno gli strumenti per evitarle, attraverso la conoscenza del fenomeno. Manca spesso la consapevolezza, tra ragazzi e adulti, che una foto o un video diffusi in rete divengono di pubblico dominio e la diffusione non è controllabile.

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.

Attraverso lezioni ed approfondimenti, riguardo all'uso dei principali social network (tik tok, snapchat, twitch, istagram, whatsapp etc.) si affronterà l'argomento e si condivideranno video ad alto impatto, per rendere chiaro agli alunni il pericoloso fenomeno del grooming.

La nostra scuola si propone di sensibilizzare genitori e alunni sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni. Per far conoscere agli studenti i rischi e i pericoli legati al grooming, saranno proiettati video della serie "se mi posti ti cancello", pubblicati su www.generazioniconnesse.it

---

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 Istituto, attraverso le attività di autoformazione e informazione, intende sensibilizzare e prevenire fenomeni legati all'uso inconsapevole delle TIC e dei social, tra i quali anche la pedopornografia. Si prevede la trattazione trasversale di temi legati all'affettività, alla sessualità e alle differenze di genere. Se si dovessero presentare dei casi, se l'entità è lieve occorre in primo luogo parlarne con alunne e alunni e le rispettive famiglie, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. Se si configurano ipotesi di reato, saranno informate le autorità competenti.

Il nostro piano d'azioni

AZIONI (da sviluppare in una annualità)

Promuovere formazione per i docenti dedicata all' Educazione Civica Digitale.

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

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.

Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.

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.

Le situazioni che dovranno essere segnalate sono le seguenti:

1. Condizioni di disagio
2. Materiali o informazioni inadeguate: foto "provocanti" o inopportune per abbigliamento o pose che possono essere oggetto di scherno o di ricatto, inviate ad amici o caricate sul profilo di un

Social Network (Sexting), oppure la pubblicazione o l'invio di messaggi violenti e offensivi.
3. Atteggiamenti poco corretti e non chiari, sia all'interno della scuola, sia al di fuori, soprattutto nel tragitto casa-scuola.

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.

Riguardo alle situazioni di lieve rilevanza si può procedere, in autonomia, con la discussione collettiva in classe. Altri casi possono essere affrontati con la convocazione di genitori e alunni, alla presenza del Referente del Cyberbullismo, per riflettere insieme sull'accaduto e individuare strategie comuni d'intervento. Nei casi più gravi e in ogni ipotesi di reato, occorre valutare tempestivamente con il Dirigente Scolastico come intervenire, convocando con urgenza i genitori.
La rilevazione avverrà attraverso la sistematica osservazione degli alunni in classe e accogliendo i bisogni dei ragazzi e delle ragazze attraverso un apposito indirizzo mail creato ad hoc:

icslombardoradicestopbullismo@gmail.com

La rilevazione dei casi è compito dell'intera comunità scolastica: docenti, studenti, personale ATA.

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

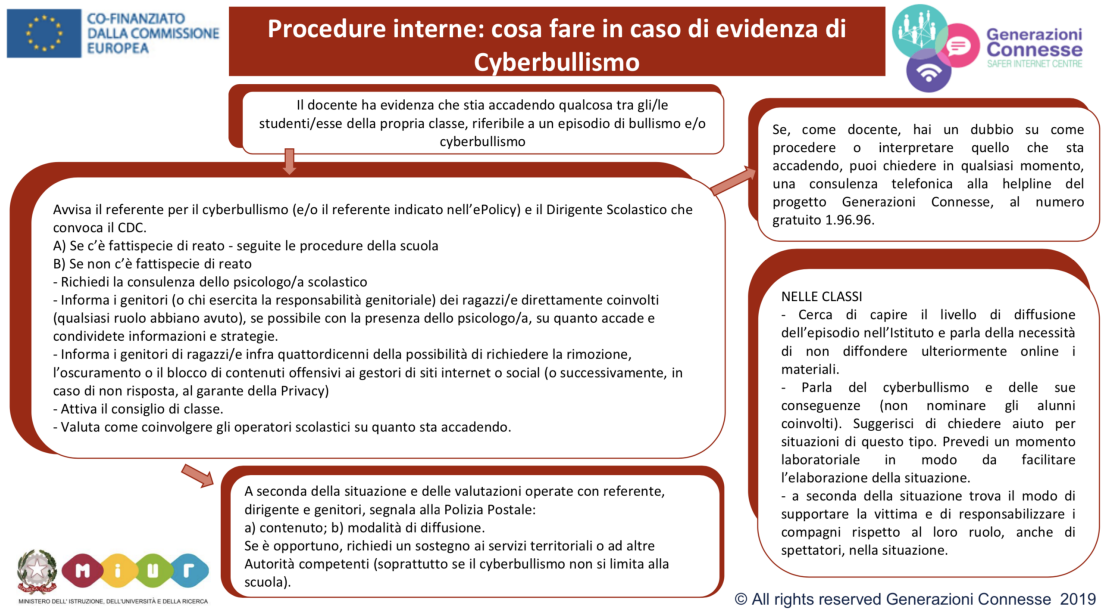
alla tutela dei minori.

- **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.

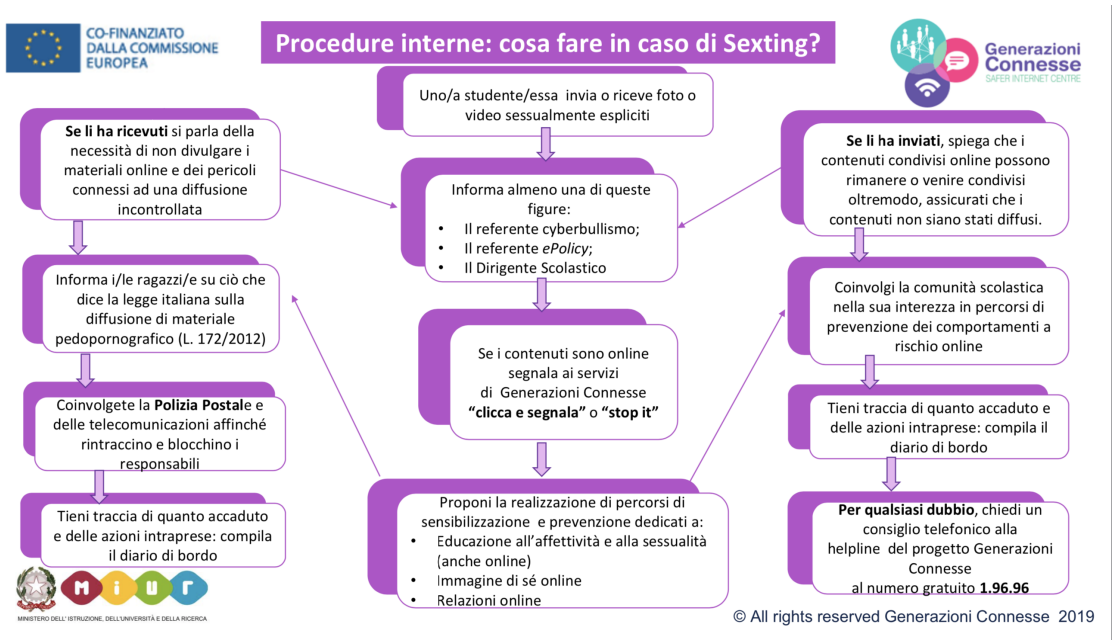
Giova ricordare che il Garante per la protezione dei dati personali ha pubblicato nel sito www.garanteprivacy.it il
MODELLO per la segnalazione/reclamo in materia di cyberbullismo da inviare a: cyberbullismo@gpdp.it. Il Garante provvede entro quarantotto ore dal ricevimento della richiesta alla rimozione, al blocco o all'oscuramento di contenuti, riferiti a un minore e diffusi per via telematica.
Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni;
- Polizia di Stato –**Commissariato Porta Nuova Ufficio** Amministrativa e Sociale
Corso Calatafimi, 421
90129 (PALERMO - PA)
Telefono: 0916561411
Stazione CC Palermo Mezzo Monreale
corso Calatafimi, 92
telefono 091488729
- Polizia di Stato – Commissariato on line (attraverso il portale http:// www.commissariatodips.it).

5.4. - Allegati con le procedure

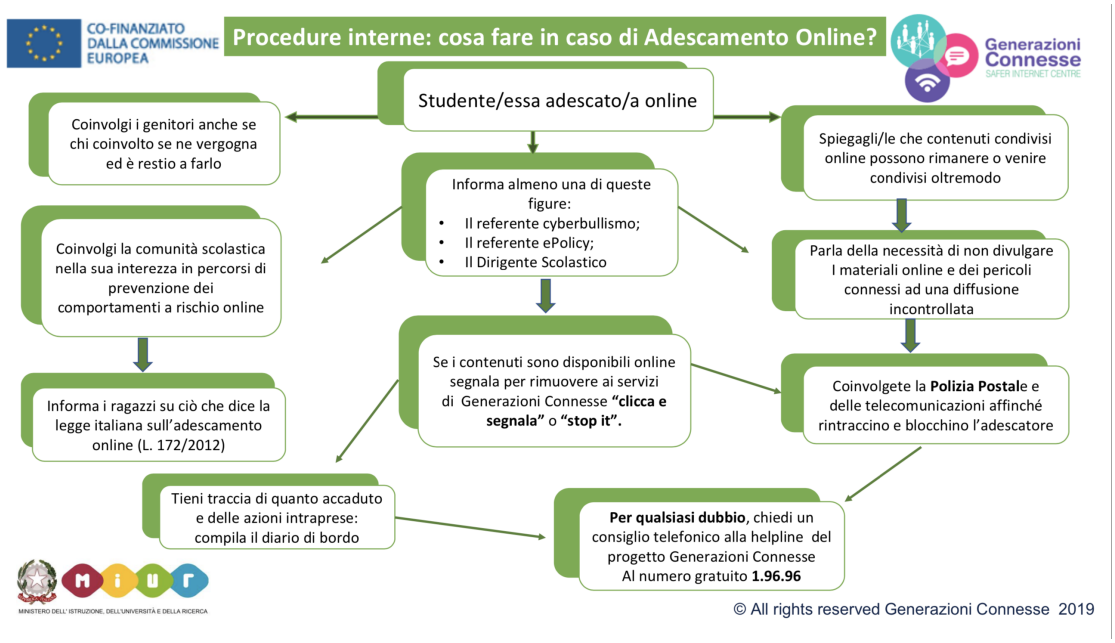
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



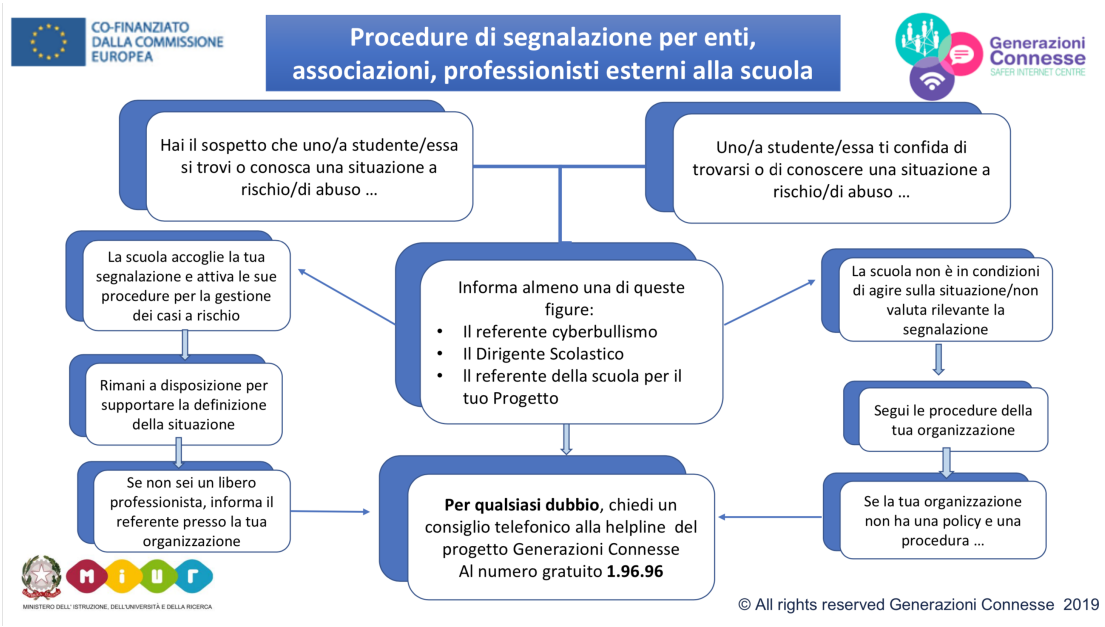
Procedure interne: cosa fare in caso di sexting?



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

Di seguito, si allega il modulo di segnalazione del nostro Istituto,

già pubblicato sul sito ufficiale della scuola

AL DIRIGENTE SCOLASTICO

AL REFERENTE BULLISMO E CYBERBULLISMO

I. C. LOMBARDO RADICE PALERMO

MODULO PER LA SEGNALAZIONE DI ATTI DI BULLISMO E/O CYBERBULLISMO

Nome Cognome di chi effettua la segnalazione (docente o genitore):

_____

Nome e cognome del minore:

_____

Classe _____Sez. _____Sede_____

In cosa consiste l'azione di bullismo/cyberbullismo di cui l'alunno si ritiene vittima? (indicare una o più opzioni nella lista che segue):

- prepotenze, minacce verbali, insulti o di altro tipo; diffusione di dicerie, esclusione dal gruppo di pari; pressioni; aggressione; molestia; ricatto; ingiuria;

- denigrazione (pubblicazione all'interno di comunità virtuali, quali blog, newsgroup, messaggistica immediata,profili facebook, di pettegolezzi e commenti crudeli, calunniosi e denigratori;

- diffamazione; flaming (litigi on line con uso di linguaggio violento e volgare);
- cyberstalking; esclusione (estromissione intenzionale dall'attività online);
- sexting (invio di messaggi via smartphone o internet, corredati da immagini a sfondo sessuali);

- furto d'identità (es: qualcuno finge di essere me sui social network, hanno rubato le mie password e utilizzato il mio account sui social network, ecc.);

- alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali (es: qualcuno ha ottenuto e diffuso immagini, video o informazioni che mi riguardano senza che io volessi, ecc.) ;

- qualcuno ha diffuso online dati e informazioni (video, foto, post, ecc.) per attaccare o ridicolizzare me, e/o la mia famiglia e/o il mio gruppo di amici.

Quali sono i contenuti che vorreste far rimuovere o oscurare sul web o su un social network? Perché li considerate atti di cyberbulismo? (inserire una sintetica descrizione – importante spiegare di cosa si tratta)

_____
_____
_____
_____
_____

Dove sono stati diffusi i contenuti offensivi? Sul sito internet [è necessario indicare l'indirizzo del sito o meglio la URL specifica] su uno o più social network [specificare su quale/i social network e su quale/i profilo/i o pagina/e in particolare] altro [specificare]. Se possibile, allegare immagini, video, screenshot e/o altri elementi informativi utili relativi all'atto di cyberbullismo e specificare qui sotto di cosa si tratta.

_____
_____
_____
_____
_____

DATA

FIRMA

Il nostro piano d'azioni

Non è prevista nessuna azione.