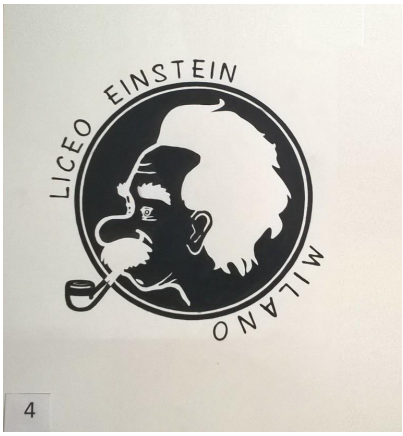


Documento di ePolicy

MIPS01000G

L.S. EINSTEIN

VIA EINSTEIN 3 - 20137 - MILANO - MILANO (MI)

Alessandra Condito

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E- policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

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

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

Argomenti del Documento

Perché è importante dotarsi di una E-policy?

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

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

Scopo del presente documento di E-policy è informare l'utenza per un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla scuola, nel rispetto della normativa vigente. In particolare, si è ritenuto importante l'avvio di un percorso diretto a sostenere docenti, personale ATA, studenti e famiglie relativamente all'utilizzo consapevole delle tecnologie digitali. La necessità di una piena consapevolezza delle potenzialità, ma anche dei rischi, legati a tali tecnologie si è rivelata imprescindibile in seguito all'introduzione della DDI (didattica digitale integrata) a causa dell'emergenza sanitaria dovuta alla pandemia Covid-19. Si ritiene, quindi, particolarmente importante specificare nel presente documento:

- le procedure e norme di comportamento riguardo l'utilizzo delle tecnologie informatiche e digitali nell'ambito delle attività legate al nostro istituto;
- le misure atte a facilitare e promuovere un utilizzo costruttivo delle TIC nella didattica, anche a distanza, e in tutto il contesto scolastico;
- le misure di prevenzione, rilevazione e gestione delle problematiche connesse ad un uso scorretto, consapevolmente o meno, delle tecnologie digitali.

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.

In particolare:

Il **Dirigente Scolastico** promuove, in sinergia con le altre figure interne ed esterne alla scuola, la cultura della sicurezza online e, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, organizza corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC. Il Dirigente Scolastico ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

L'**Animatore Digitale** supporta il personale scolastico da un punto di vista tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali. È, inoltre, uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale". Monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola.

Il **Referente bullismo e cyberbullismo**, in base all'art. 4 Legge n.71/2017, "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo" ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può avvalersi della collaborazione di Enti di formazione, Università, Forze di polizia, associazioni e centri di aggregazione giovanile del territorio. Coinvolge, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.

I **docenti** hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete, eventualmente integrando parte del curricolo con moduli specifici sulla cittadinanza digitale, anche valorizzando l'apporto dell'educazione civica e sensibilizzando gli studenti al tema delle potenzialità offerte dalle TIC e dalla rete Internet, al rispetto della privacy e del diritto d'autore. I docenti sono tenuti a segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

Il **personale Amministrativo, Tecnico e Ausiliario** (ATA) svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il Dirigente Scolastico e con il personale docente tutto. Diverse figure che, in sinergia, si occupano ciascuno per la propria funzione, del funzionamento dell'Istituto Scolastico che passa anche attraverso lo sviluppo della cultura digitale. Una collaborazione preziosa in tal senso è data dall'assistente tecnico informatico.

Studenti e studentesse hanno il compito, in relazione al proprio grado di maturità e consapevolezza raggiunta, di utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; di adottare condotte rispettose degli altri anche quando si comunica in rete, facendosi promotori di quanto appreso anche attraverso possibili percorsi di *peer education*.

Genitori e tutori, in collaborazione con le figure appartenenti all'Istituto Scolastico, sono parte attiva nella promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei *device* personali. Compito della famiglia è di attivare un controllo verso siti web non certificati (giochi, scommesse, *deep web*), social media con pubblicazione foto e video che possano compromettere il benessere dei propri figli o dei loro compagni o amici.

Gli **Enti educativi esterni e le associazioni**, che entrano in relazione con la scuola, hanno il compito di conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC, garantendo la sicurezza online degli studenti e delle studentesse durante le attività che si svolgono insieme.

Responsabile della Protezione dei Dati

Sui temi legati alla tutela della privacy la scuola ha nominato il Responsabile della Protezione dei Dati (RPD o DPO) raggiungibile al seguente indirizzo: L.S.S. "A. Einstein" – Responsabile della Protezione dei dati personali, Via A. Einstein 3, 20137 Milano, e-mail: privacy@liceoeinsteinmilano.edu.it

---

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, essere guidati dal principio di interesse superiore del minore.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse.

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). In particolare, tutti gli attori esterni sono tenuti a conoscere e rispettare la PUA di Istituto.

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 pubblicato sul sito 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.

INFRAZIONI DISCIPLINARI PER USO IMPROPRIO DELLE TIC E DELLA RETE A SCUOLA

Tutte le infrazioni dovranno essere tempestivamente segnalate a un docente, o direttamente al Dirigente Scolastico. Qualora la segnalazione venga fatta ai docenti, questi sono tenuti a riferire l'accaduto al Dirigente.

INFRAZIONI DISCIPLINARI RIGUARDANTI ATTI DI CYBERBULLISMO

Sono da considerarsi atti di cyberbullismo:

- **la condivisione online di immagini o video di compagni/e che li ritraggono in pose umilianti e denigratorie;**
- **la condivisione di scatti intimi e a sfondo sessuale; l'invio di immagini o video volti all'esclusione di compagni/e.**

Tali infrazioni saranno sanzionate sulla base di quanto previsto nel Regolamento d'Istituto. Valutata la natura e la gravità di quanto accaduto, inoltre, potrebbe rendersi necessario **denunciare l'episodio** alle forze dell'Ordine e/o garantire immediato supporto psicologico allo/la studente/ssa attraverso i servizi predisposti.

Ulteriori e dettagliate informazioni sulla valutazione e gestione dei casi di bullismo e cyberbullismo sono inserite all'interno del Protocollo d'Emergenza, consultabile sul sito dell'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.

Il presente documento integra quanto contenuto nella PUA (Politica d'uso accettabile e sicuro della rete e Regolamento di accesso e utilizzo delle risorse tecnologiche) e negli altri Regolamenti vigenti all'interno dell'Istituto.

1.7 – Monitoraggio dell'implementazione della e-Policy 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. Il monitoraggio del documento sarà realizzato a cura del Docente referente per la prevenzione e il contrasto al bullismo e cyberbullismo in collaborazione con il Dirigente Scolastico e il Vicepreside, a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone. Le modifiche del documento saranno discusse negli Organi Collegiali.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.

Azioni da svolgere nei prossimi 3 anni:

- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
- Organizzare 1 evento di presentazione e conoscenza dell'e-Policy 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.

Competenze da promuovere:

"Alfabetizzazione e dati"

L'area promuove lo sviluppo delle seguenti competenze: 1. Navigare, ricercare e filtrare dati, informazioni e contenuti digitali; 2. Valutare e gestire dati, informazioni e contenuti digitali; 3. Saper riconoscere e sapersi difendere da contenuti dannosi e pericolosi in Rete (es. app, giochi online, siti non adatti ai minori, materiale pornografico e pedo-pornografico etc.).

"Comunicazione e collaborazione"

Quest'area fa riferimento a quelle competenze volte a riconoscere le giuste ed appropriate modalità per comunicare e relazionarsi online: 1. Saper interagire con gli altri attraverso le tecnologie digitali; 2. Essere consapevoli nella condivisione delle informazioni in Rete; 3. Essere buoni "cittadini digitali"; 4. Collaborare adeguatamente con gli altri attraverso le tecnologie digitali; 5. Conoscere le "Netiquette", ovvero le norme di comportamento online; 6. Saper gestire la propria "identità digitale".

"Sicurezza"

Quest'area include l'imprescindibilità di salvaguardare i propri dati personali e rispettare le regole nel trattare i dati altrui e promuove le seguenti competenze: 1. Imparare a proteggere i dispositivi e i contenuti digitali e comprendere i rischi e le minacce presenti negli ambienti digitali. Conoscere le misure di sicurezza e protezione; 2. Proteggere i dati personali e la privacy negli ambienti digitali. Capire come utilizzare e condividere informazioni personali, proteggendo se stessi e gli altri dai danni; 3. Conoscere ed esercitare i propri diritti in termini di privacy e sicurezza.

Studenti e famiglie sono chiamati a partecipare alle iniziative di sensibilizzazione sul corretto uso delle tecnologie digitali sia sulle potenzialità della Rete.

Agli studenti sono proposte diverse iniziative, quali: *Hackathon* contro il cyberbullismo, progetti *peer-to-peer* realizzati a partire dai materiali messi a disposizione dal *Safer Internet Centre*, eventi dedicati al tema. Per le famiglie sono previsti annualmente incontri con il docente referente per la prevenzione e il contrasto del bullismo e cyberbullismo e lo psicologo d'istituto.

Sul sito della scuola, in un'area dedicata, è possibile trovare materiali e link utili per approfondimenti, spunti aggiornamenti e strumenti didattici sul tema dei rischi in Rete utili a studenti/esse, docenti e famiglie.

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.

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

Per realizzare ciò, il nostro Istituto offre ai propri docenti corsi di formazione e aggiornamento in merito all'utilizzo e l'integrazione delle TIC. La formazione è promossa sia dalla scuola, con l'aiuto dell'animatore digitale, sia dalle reti di scuole e dall'amministrazione.

L'attenzione del nostro istituto all'uso delle TIC nella didattica va inserita nell'ottica di guidare le studentesse e gli studenti verso una fruizione e selezione dei contenuti online critica e consapevole.

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 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.

Allo scopo di creare ulteriore sinergia fra scuola, studenti/sse e famiglie, di promuovere la condivisione di buone pratiche nell'utilizzo consapevole delle TIC e di prevenire e contrastare ogni forma di discriminazione, offesa, denigrazione e lesione della dignità dell'altro, nonché fenomeni di bullismo e cyberbullismo, il nostro Istituto promuoverà incontri formativi specifici che abbiano ad oggetto l'uso responsabile e sicuro della Rete.

Il team dell'Epolicy realizzerà un'area specifica sul sito dell'Istituto con materiali formativi per gli insegnanti.

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 i/le ragazzi/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del Regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.
Al seguente link è possibile consultare tutte le attività, le iniziative promosse dal nostro istituto, i riferimenti utili per un uso responsabile e consapevole degli strumenti digitali e i contatti per il supporto o eventuali segnalazioni:

https://www.liceoeinsteinmilano.edu.it/29377-2/

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021)

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

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

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie 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 degli studenti e delle 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.

Il nostro Istituto, in linea con quanto stabilito per le istituzioni scolastiche pubbliche, tratta solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali, oppure quelli espressamente previsti dalla normativa di settore. Per tali trattamenti non è necessario il consenso degli/lle studenti/esse.

Alcune categorie di dati personali degli/lle studenti/esse e delle famiglie, come quelli sensibili e giudiziari, sono trattati con estrema cautela, nel rispetto di specifiche norme di legge, verificando non solo la pertinenza e completezza dei dati, ma anche la loro indispensabilità rispetto alle "finalità di rilevante interesse pubblico" che si intendono perseguire.

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.

Il nostro Istituto è raggiunto dalla fibra ottica, sufficientemente veloce da permettere l'uso di soluzioni *cloud* per la didattica e l'uso di contenuti di apprendimento multimediali (come previsto dal PNSD - Piano Nazionale Scuola digitale). Ogni aula è dotata di pc e videoproiettore, 10 delle nostre aule sono dotate di LIM e sono presenti due laboratori di informatica. Particolare attenzione è dedicata alla dematerializzazione degli atti e delle comunicazioni tra dirigenti, docenti, famiglie e studenti/esse, effettuate per mezzo mail e/o registro elettronico.

Con l'introduzione della DDI, il nostro Istituto ha fornito dispositivi digitali in comodato d'uso (pc e tablet) a tutti gli/le studenti/esse che ne hanno fatto richiesta. Al fine di garantire il diritto di accesso a internet e a partire dall'analisi dei bisogni della scuola, abbiamo garantito e continueremo a garantire interventi mirati per il superamento di ogni forma di divario digitale determinato dalle condizioni economiche delle famiglie degli/lle studenti/studentesse.

Cybersecurity

Il Liceo Einstein garantisce:

- **La separazione delle reti didattica e segreteria:** ciò è importante per garantire maggiore sicurezza alle informazioni, gestendo in modo autonomo e con regole differenti le due reti grazie al firewall.
- **L'aggiornamento periodico di software e Sistema operativo:** garantisce che il sistema sia aggiornato e protetto dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo.
- **la programmazione di backup periodici:** cioè la copia e messa in sicurezza dei dati del sistema scolastico per prevenire la perdita degli stessi.
- **la formazione adeguata ai docenti:** la formazione riguarda la gestione dei dispositivi, la conoscenza delle regole basilari sulla sicurezza.
- **il regolare controllo sulle possibili vulnerabilità.**

Si rimanda alla PUA "Politica di Uso Accettabile delle tecnologie a scuola" per i riferimenti in merito a:

- accesso alle postazioni in rete della scuola dei diversi soggetti operanti nell'Istituto: personale in servizio, allievi, eventuali soggetti esterni alla scuola
- accesso ai servizi resi disponibili sui computer in rete dei diversi soggetti operanti nell'Istituto
- garanzie a tutela della privacy nell'uso degli strumenti tecnologici d'Istituto

L'istituto, inoltre, attraverso l'adozione di sistemi di filtraggio software e hardware, inibisce l'accesso online da parte di studenti/esse a materiali non adeguati alla loro fascia d'età.

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.

Il Liceo Einstein, attraverso il frequente aggiornamento del sito web istituzionale, garantisce una costante comunicazione online al fine di:

- valorizzare e promuovere attività, progetti e finalità dell'offerta formativa all'utenza e agli enti esterni (Università, associazioni, istituzioni) garantire la diffusione di
- informazioni di servizio o contenuti importanti fra docenti, studenti, genitori, personale ATA

La comunicazione esterna e interna dell'Istituto è implementata anche con il supporto degli studenti che producono contenuti multimediali da diffondere attraverso i vari canali in uso (video, foto, articoli per il sito).

Tra gli strumenti di comunicazione interna, oltre il sito, l'Istituto si avvale del registro elettronico in uso da 7 anni

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

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

Come stabilito dall'articolo 3 del D.P.R. n. 249/1998 è previsto:

"per ciascuno studente, di non utilizzare il telefono cellulare, o altri dispositivi elettronici, durante lo svolgimento delle attività didattiche, considerato che il discente ha il dovere:

- di assolvere assiduamente agli impegni di studio durante gli orari di lezione (comma 1)
- di tenere comportamenti rispettosi degli altri (comma 2), nonché corretti e coerenti con i principi di cui all'art. 1 (comma 3)
- di osservare le disposizioni organizzative dettate dai regolamenti di istituto (comma 4)" (DM n. 30 del 15/03/2007 - "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, doveri di vigilanza e di corresponsabilità dei genitori e dei docenti").

Nel nostro Regolamento d'Istituto sono specificate le sanzioni disciplinari in caso di uso scorretto dei cellulari da parte degli studenti/sse durante le attività didattiche e all'interno dell'Istituto.

L'Istituto non trascura però l'aspetto inclusivo e creativo delle tecnologie digitali come strumenti da inserire nella didattica (es. consultare in classe libri digitali e testi online) e nelle attività laboratoriali. L'uso viene consentito per scopi prettamente didattici, sotto il controllo e la responsabilità del docente che pianifica l'attività. Come si legge nel Piano Nazionale Scuola Digitale emanato dal MIUR con la Legge 107 del 2015: "al fine di sviluppare e di migliorare le competenze digitali degli studenti e di rendere la tecnologia digitale uno strumento didattico di costruzione delle competenze in generale, il Ministero dell'istruzione, dell'università e della ricerca adotta il Piano nazionale per la scuola digitale (...)".

In tal senso, gli smartphone, i tablet e i pc personali possono essere integrati dai nostri docenti nel lavoro nelle classi quando ben progettato e calibrato per discipline e obiettivi formativi. Il docente ha comunque il compito di vigilare affinché gli/le studenti/sse facciano un uso corretto dei dispositivi digitali.

In riferimento alla Legge n. 71 del 2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", il nostro Istituto coinvolge attivamente, con diverse iniziative nell'arco dell'anno scolastico, docenti, genitori e studenti/esse con incontri mirati, attività *peer-to-peer* e iniziative volti a contrastare abusi, attacchi verbali, la messa in ridicolo degli/lle studenti/esse attraverso le tecnologie digitali. ln particolare, il progetto HACKATHON regionale sul cyberbullismo, la piattaforma Generazioni Connesse e la collaborazione con l'Università Bicocca di Milano ci hanno permesso di avviare iniziative finalizzate a fornire informazioni, materiali e spunti utili per avviare un processo educativo e didattico che ha visto coinvolti docenti, studenti/esse e famiglie.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021).

- 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)

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

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi
- digitali personali Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

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 mette in atto interventi di sensibilizzazione e prevenzione con l'obiettivo di accrescere la consapevolezza presso gli/le studenti/sse, i docenti e le famiglie dei rischi derivanti da un uso non consapevole del digitale e della Rete. Se le Tecnologie dell'Informazione e della Comunicazione (TIC) sono parte integrante della vita quotidiana dei più giovani, sia come strumenti privilegiati di comunicazione e di

relazione, ma anche di informazione, studio e partecipazione, esse pongono però delle questioni associate alla sicurezza e al comportamento sociale. Si rende necessario, quindi, soprattutto nei più giovani (classi del primo biennio), promuovere competenze base e strumenti critici al fine di garantire loro una preparazione adeguata sull'uso delle TIC volta a sfruttarne le potenzialità e gestirne le implicazioni.. Avvalendoci del supporto di risorse interne all'istituto (docenti, psicologo) e di risorse esterne (Università, associazioni), offriamo agli studenti/esse stimoli, strumenti e conoscenze atti a consolidare quelle competenze educative di base necessarie a poter gestire le situazioni di vita che i/le ragazzi/e 36sperimentano online.

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 ai minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.

- **Il Referente per le iniziative di prevenzione:**
  - 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).

I genitori hanno il dovere di educare e vigilare, in maniera adeguata all'età del figlio, cercando di correggerne comportamenti a rischio. Questa responsabilità persiste anche per atti compiuti in orario scolastico.

La scuola ha il dovere di intervenire tempestivamente laddove venga a conoscenza di comportamenti a rischio, mettendo in atto misure a tutela dei minori coinvolti e promuovendo azioni formative opportune.

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 è 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, anche grazie all'apporto dell'insegnamento di Educazione Civica, contribuisce al raggiungimento degli obiettivi sopra descritti.

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.

Gran parte delle attività proposte sull'uso consapevole della rete sono tesi a promuovere una cultura digitale, intesa come capacità di creare e mantenere una relazione sana con la tecnologia.

Il nostro Istituto, inoltre, presta particolare attenzione ai segnali comportamentali degli/lle

studenti/esse (es. un'attenzione eccessiva al gioco online e/o all'abuso di navigazione in Rete).

In caso di rilevazione o segnalazione (da parte di un docente, di uno studente…) il piano di intervento prevede:

- la comunicazione tempestiva ai genitori di quanto rilevato o segnalato
- l'organizzazione di incontri rivolti alle famiglie presieduti dalla Dirigente, con il supporto del docente referente per la prevenzione e il contrasto al bullismo e cyberbullismo e/o dello psicologo d'Istituto
- la definizione e l'entità del problema le
- possibili soluzioni
- incontri periodici per il monitoraggio

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).

I contenuti sessualmente espliciti possono diventare materiale di ricatto attraverso la 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.

La diffusione di contenuti personali, attraverso video e/o foto, può danneggiare, sia in termini psicologici che sociali, sia il/la ragazzo/a presente nella foto/video che i soggetti che hanno contribuito a diffonderla.

Gli/le studenti/esse e le famiglie coinvolti in un caso, anche solo presunto, di *sexting* possono rivolgersi alle autorità competenti e/o alla Dirigente Scolastica, ai docenti o usufruire del supporto dello sportello di ascolto psicologico.

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 gli/le studenti/esse in un percorso di educazione all'affettività e alla sessualità. Il nostro Istituto da alcuni anni ha attivato un progetto di educazione sessuale rivolto alle classi seconde per aiutare i ragazzi più giovani a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri.

Nel caso in cui studenti/esse fossero vittime, o sospette tali, di un caso di adescamento online è importante che l'adulto di riferimento non si sostituisca al minore nel rispondere all'adescatore e che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove.

I casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile.

L'adescamento, inoltre, può avere ripercussioni psicologiche significative su ragazzi molto giovani e per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima un adeguato supporto psicologico.

Per consigli e per un supporto è possibile rivolgersi alla Helpline di Generazioni Connesse (19696): operatori esperti e preparati sono sempre a disposizione dei docenti, del Dirigente e degli operatori scolastici, oltre che degli/lle studenti/sse, dei genitori/tutori.

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.**

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.

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.

Per maggiori approfondimenti, si invita a fare riferimento al Vademecum di Generazioni Connesse.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021).

Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

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

Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

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

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

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

Questa sezione dell'e-Policy 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**.

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 incontri che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola e attraverso news nel sito della scuola.

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. 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.

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.

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 prevede alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;
- 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.

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.

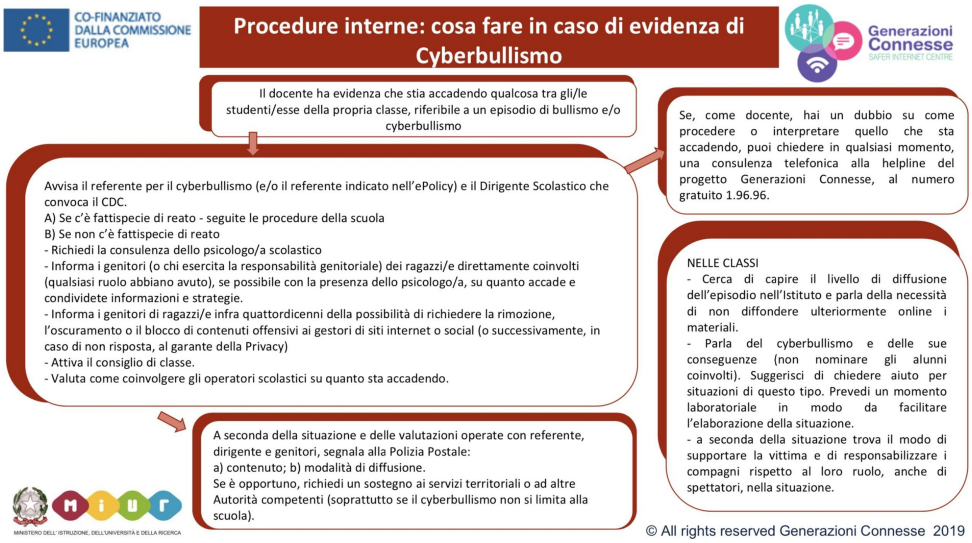
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **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.

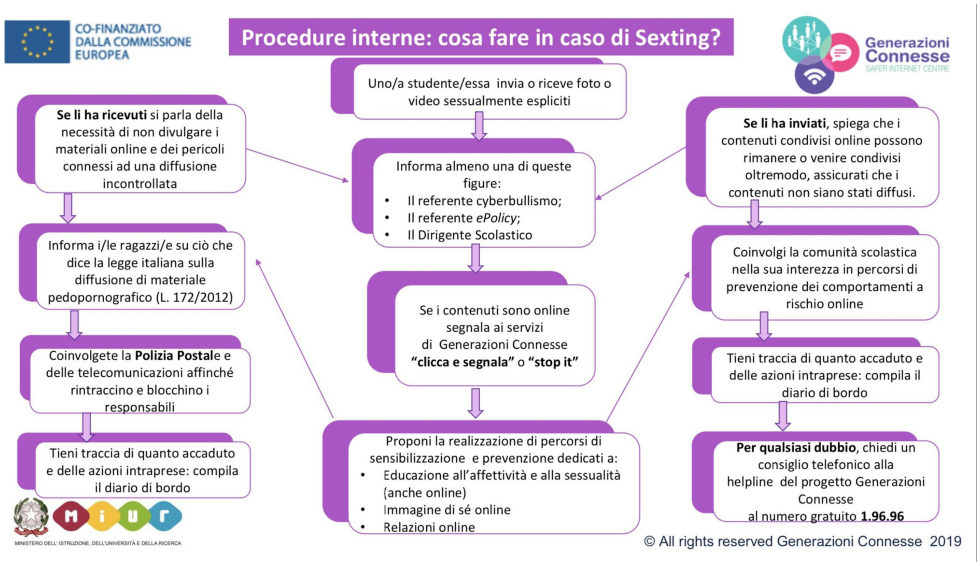
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

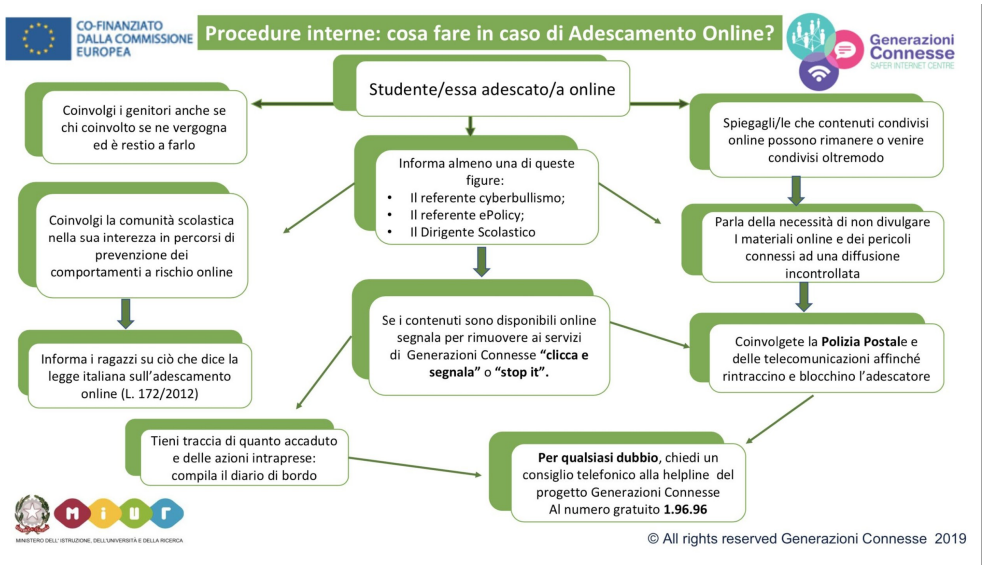
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



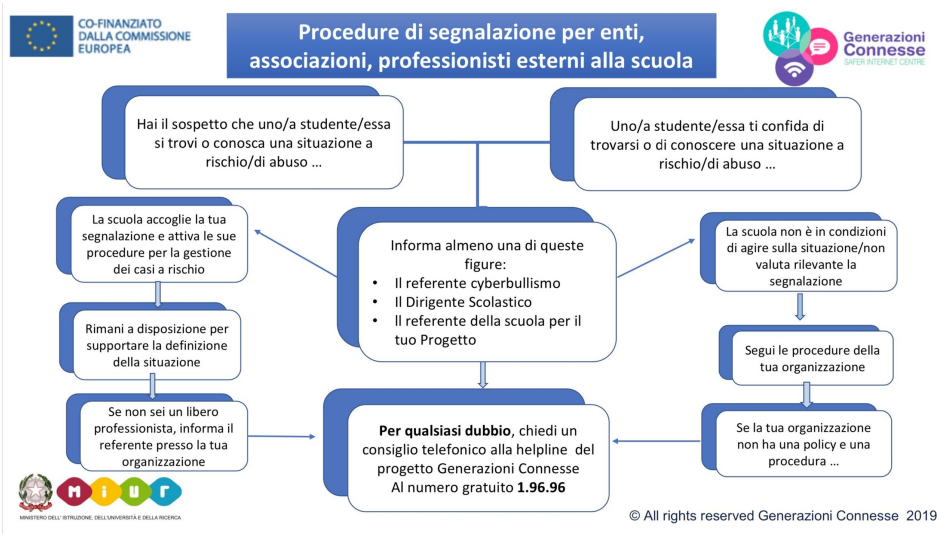
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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


CO-FINANZIATO DALLA COMMISSIONE EUROPEA
Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola
Generazioni Connesse
Hai il sospetto che uno/a studente/essa si trovi o conosca una situazione a rischio/di abuso …
Uno/a studente/essa ti confida di trovarsi o di conoscere una situazione a rischio/di abuso …
La scuola accoglie la tua segnalazione e attiva le sue procedure per la gestione dei casi a rischio
Rimani a disposizione per supportare la definizione della situazione
Se non sei un libero professionista, informa il referente presso la tua organizzazione
Informa almeno una di queste figure:
• Il referente cyberbullismo
• Il Dirigente Scolastico
• Il referente della scuola per il tuo Progetto
La scuola non è in condizioni di agire sulla situazione/non valuta rilevante la segnalazione
Segui le procedure della tua organizzazione
Se la tua organizzazione non ha una policy e una procedura …
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse Al numero gratuito 1.96.96
MIUR
© All rights reserved Generazioni Connesse 2019