Documento di ePolicy

BAIC89400E

I.C. "DE AMICIS-GIOVANNI XXIII"

P.ZZA DI VAGNO 18 - 70021 - ACQUAVIVA DELLE FONTI - BARI (BA)

VALERIA BRUNETTI

Firmato da:
BRUNETTI VALERIA
12/12/2021 17:56:20

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

1.2 - Ruoli e responsabilità

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

Dirigente scolastico:

- Garantisce la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- Garantisce ai propri docenti una formazione di base sulle tecnologie dell'Informazione e della Comunicazione (ICT) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse;
- Garantisce l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on- line;
- Informa tempestivamente, qualora venga a conoscenza di atti di cyberbullismo che non si configurino come reato, i genitori dei minori coinvolti; (o chi ne esercita la responsabilità genitoriale o i tutori)
- Regola il comportamento degli studenti ed impone sanzioni disciplinari in caso di comportamento inadeguato.

Referente Cyberbullismo d'Istituto:

- Coordina iniziative di prevenzione e contrasto del cyberbullismo messe in atto dalla scuola;
- Predispone un documento di rilevazione di incidenti di sicurezza in rete;
- Facilita la formazione e la consulenza di tutto il personale.

Animatore digitale e Team dell'innovazione:

- Pubblicano il presente documento di E-Safety Policy sul sito della scuola;
- Diffondono i contenuti del documento tra docenti e studenti.

Insegnanti:

- Provvedono personalmente alla propria formazione/aggiornamento sull'utilizzo

del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in internet e dell'immagine degli altri: lotta al cyberbullismo);
- Supportano gli alunni nell'utilizzo consapevole delle tecnologie informatiche utilizzate a scopi didattici;
- Segnalano al Dirigente Scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazione;
- Supportano ed indirizzano alunni coinvolti in problematiche legate alla rete.

Direttore dei Servizi Generali e Amministrativi:

- Assicura, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione necessari ad evitare un cattivo funzionamento della dotazione Tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate.

Genitori:

- Contribuiscono, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- Incoraggiano l'impiego delle ICT da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga in sicurezza;
- Agiscono in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite;
- Rispondono per gli episodi commessi dai figli minori a titolo di culpa in educando (articolo 2048 del Codice Civile). Sono esonerati da responsabilità solo se dimostrano di non aver potuto impedire il fatto. Nei casi più gravi i giudici per l'inadeguatezza dell'educazione impartita ai figli emerge dagli stessi episodi di bullismo, che per le loro modalità esecutive dimostrano maturità ed educazione carenti.

Gli Enti educativi esterni e le associazioni:

- Osservano le politiche interne sull'uso consapevole della Rete e delle TIC;
- attivano procedure e comportamenti sicuri per la protezione degli studenti e delle studentesse durante le attività che vengono svolte all'interno della scuola o in cui sono impegnati gli stessi.

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

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 attività progettuali e di formazione devono essere preventivamente autorizzate dal Dirigente scolastico, con modalità e tempi concordati.

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

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/lle studenti/esse) si faccia a sua volta promotore del documento.

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

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

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

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

L'ePolicy deve essere condivisa attraverso i docenti curricolari, con gli studenti, per dare loro una base di partenza per un uso consapevole e maturo dei dispositivi e della tecnologia informatica e soprattutto regole condivise di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici; l'ePolicy deve dare loro elementi per poter riconoscere e quindi prevenire comportamenti a rischio sia personali che dei propri compagni. L'ePolicy deve essere condivisa con il personale scolastico e con i genitori attraverso il sito istituzionale della scuola e il riferimento alla stessa nel patto di corresponsabilità.

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.

Le sanzioni saranno:

- Richiamo verbale;
- Sanzioni commisurate alla gravità della violazione commessa;
- Nota informativa ai genitori o tutori mediante registro elettronico;
- Convocazione dei genitori o tutori per un colloquio con l'insegnante;
- Convocazione dei genitori o tutori per un colloquio con il Dirigente Scolastico.

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 e-Policy è coerente con quanto stabilito nei Regolamenti vigenti e nel Patto di corresponabilità.

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 monitoraggio e la revisione della e-Policy sarà svolta annualmente e /o qualora si verifichino cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno dell'Istituto.
L'aggiornamento del documento di e-Policy sarà curato dal docente Referente di Istituto per la prevenzione e il contrasto del bullismo e cyberbullismo, in qualità di coordinatore del gruppo di lavoro del presente documento e, ove possibile, con la partecipazione dell'Animatore Digitale.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare un'attività di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare un'attività di presentazione e conoscenza dell'ePolicy

rivolto ai genitori
- Organizzare un'attività di presentazione e conoscenza dell'ePolicy rivolto agli studenti

Azioni da svolgere nei prossimi 3 anni:

- Organizzare attività di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 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.

Le finalità formative delle TIC possono essere sintetizzate nei seguenti punti:
-Favorire la conoscenza dello strumento pc e/o tablet a scopo didattico
-Sostenere l'alfabetizzazione informatica
-Favorire la trasversalità delle discipline
-Facilitare il processo di apprendimento
-Favorire il processo di inclusione
-Fornire nuovi strumenti a supporto dell'attività didattica
-Promuovere situazioni collaborative di lavoro e di studio
-Sviluppare creatività e capacità di lavorare in gruppo
-Promuovere azioni di cittadinanza attiva
-Utilizzare in modo critico, consapevole e collaborativo la tecnologia.
Competenze digitali declinate secondo le cinque aree del quadro di riferimento DIGCOM (Quadro comune di riferimento europeo per le competenze digitali):
1. INFORMAZIONE: identificare, localizzare, recuperare, conservare, organizzare e

analizzare le informazioni digitali, giudicare la loro importanza e lo scopo;
2. COMUNICAZIONE: comunicare in ambienti digitali, condividere risorse attraverso strumenti on-line, collegarsi con gli altri e collaborare attraverso strumenti digitali, interagire e partecipare alle comunità e alle reti;
3. CREAZIONE DI CONTENUTI: creare e modificare nuovi contenuti (da elaborazione testi a immagini e video); integrare e rielaborare le conoscenze ed i contenuti; produrre espressioni creative, contenuti media e programmare; conoscere e applicare i diritti di proprietà intellettuale e le licenze;
4. SICUREZZA: protezione personale, protezione dei dati, protezione dell'identità digitale, misure di sicurezza, uso sicuro e sostenibile;
5. PROBLEM-SOLVING: identificare i bisogni e le risorse digitali, valutare appropriati strumenti digitali secondo lo scopo o necessità, risolvere problemi concettuali attraverso i mezzi digitali, utilizzare creativamente le tecnologie, risolvere problemi tecnici, aggiornare la propria competenza e quella altrui.

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.

La competenza digitale è imprescindibile sia per i docenti sia per gli studenti e per le studentesse, e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa ed in grado di venire incontro ai nuovi stili di apprendimento.

Il nostro Istituto riconosce e favorisce la partecipazione del personale ad iniziative coerenti con il piano di formazione indicato nel PTOF.

2.3 - Formazione dei docenti

sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

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

I momenti di formazione ed aggiornamento sono formulati secondo un'analisi del fabbisogno formativo del corpo docente sull'utilizzo sicuro di Internet e delle tecnologie digitali

---

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.

Oggi più che mai è importante rinforzare l'alleanza educativa fra scuola e famiglie. Sarebbe opportuno aggiornare o integrare, oltre che il regolamento scolastico, anche il "Patto di corresponsabilità", con specifici riferimenti alle tecnologie digitali e all'ePolicy, per informare e rendere partecipi le famiglie. A tale proposito è importante informare i genitori sulle condotte che si dovranno adottare a scuola e, in generale,

offrire loro consigli da mettere in pratica con i propri figli, in riferimento ai rischi connessi ad un uso distorto della Rete da parte degli studenti.

Il nostro piano d'azioni

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

- 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.

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

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

Il nostro Istituto, in relazione al trattamento dei dati, ha dedicato una sezione "Privacy" sul sito web dell'Istituto. Sono pubblicati i seguenti documneti:

- Informativa del Regolamento Europeo 2016/679, per il trattamento dei dati personali degli alunni e delle famiglie;

- Informativa ex art. 13 D.Lgs. n.196/2003 e ex art. 13 del Regolamento Europeo 2016/679, per il trattamento dei dati personali dei dipendenti;

- Informativa ex art. 13 D.Lgs. n.196/2003 e ex art. 13 del Regolamento Europeo 2016/679, per il trattamento dei dati dei fornitori dell'Istituto;

- Informativa sul trattamento dei dati FAD/DAD;

- Informativa_Privacy_per_Didattica_a_distanza: Attivazione modalità didattiche a distanza (FAD/DAD) per emergenza COVID-19;

- Informativa Privacy ex artt. 13 e 14 del Regolamento UE 2016/679, per il trattamento dei dati personali ai fini dell'iscrizione ed utilizzo delle piattaforme digitali e "Google Suite for Education"

- Informativa per DIPENDENTI, ALUNNI e FAMIGLIE, UTENTI su misure anti contagio da COVID-19 (rilevazione della temperatura corporea) (artt. 13-14 Regolamento UE 2016/679 – DPCM 26/4/2020);

- Raccomandazione e indicazioni per la sicurezza degli utenti per prevenire attacchi informatici;

- Raccomandazioni di sicurezza per l'Utente (smart working.

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 rete wi-fi è protetta da password in possesso dei docenti che utilizzano quotidianamente i dispositivi digitali all'interno delle classi per l'uso del registro elettronicoe e per la didattica. I dispositivi BYOD degli alunni delle classi digitali della scuola secondaria di primo grado, all'inizio del triennio vengono connessi alla rete wifi del plesso dall'animatore digitale e dai docenti del Team digitale in fase di Startup.
Le operazioni di gestione, configurazione, backup e ripristino sono affidate a un tecnico esterno.

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.

Posta elettronica

Tutti i docenti dell'istituto sono dotati di un indirizzo di posta elettronica della scuola del tipo: inizialenome.cognomed@icdeamicisgiovanni23.edu.it. per la gestione della comunicazione interna, e della didattica digitale integrata e DAD.

Gli alunni, della scuola primaria e della scuola secondaria di primo grado sono dotati di un indirizzo di posta elettronica della scuola del tipo:

inizialenome.cognomes@icdeamicisgiovanni23.edu.it.

per l'utilizzo delle attività didattiche digitali integrate e per la DaD . La dotazione di indirizzi di postaelettronica sia dei docenti che degli alunni appartiene all'infrastruttura delle Google Suite for Education.

Sito web e pagina Facebook della scuola.

La scuola ha un sito web e una pagina Facebook,quest'ulitma gestita dai docenti FS, di cui è responsabile dove vengono pubblicati i contenuti valutati come pertinenti alle finalità educative istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative.

Registro elettronico

Da qualche anno è in uso il Registro Elettronico, accessibile ai genitori, utilizzato dai docenti per la registrazione delle attività didattiche e delle valutazioni, e dal dirigente scolastico e dai docenti coordinatori di classe per le comunicazioni scuola-famiglia.

3.4 - Strumentazione personale

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

queste il Progetto Generazioni Connesse e il più ampio PNSD.

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

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

Ogni docente è responsabile del proprio username e della propria password di accesso al registro elettronico e delle password d'accesso alla rete wifi dell'Istituto. In caso di smarrimento o dimenticanza i docenti devono rivolgersi alla segreteria e far presente il problema. A tutto il personale, docente e non docente, è stato raccomandato di non salvare le password nei browser se gli strumenti vengono utilizzati da più persone e di effettuare sempre il logout dai siti a cui si accede con login e dalle caselle di posta personali. In ogni caso è consigliata la navigazione in modalità incognito del browser sulle periferiche della scuola (PC, notebook, tablet, ecc.).

Si invitano altresì i docenti ad una custodia responsabile di tutte le credenziali di accesso con password segrete, alfanumeriche e sicure, cambiate almeno ogni tre mesi.

Il nostro piano d'azioni

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

- 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 a scuola
- Organizzare uno o più eventi o attività volti a formare il personale dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

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

Scegliere almeno 1 di queste azioni:

- 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 il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

Gli interventi di sensibilizzazione e prevenzione dei rischi online verranno implementati su più livelli:

INTERVENTI LIVELLO SCUOLA:(Prevenzione Universale)

1) formazione di un team d'intervento adeguatamente formato

2) implementazione sulla home page del sito dell'Istituto di una sezione specifica dedicata

3) Creazione di una banca dati (libri, riviste, filmografia, siti web) relativa al fenomeno alle possibili strategie d"intervento.

4) Costante attività di vigilanza da parte di tutto il personale scolastico.

5) Attività formative rivolte ai docenti.

6) Coinvolgimento delle famiglie nei programmi contro rischi della rete attivati dalla scuola attraverso incontri informativi.

7) Collaborazione con le Forze dell'Ordine e con enti e associazioni esterni

8) Incontri con gli alunni, anche tramite l'intervento di testimonial e proiezione di filmati.

9) Elaborazione di questionari per il monitoraggio del fenomeno.

10) Promozione dell'educazione all'uso consapevole della rete internet e ai diritti e ai doveri connessi all'utilizzo delle tecnologie informatiche quale elemento trasversale alle diverse discipline curricolari.

11) Individuazione di semplici regole comportamentali .

Inoltre, rientra in un approccio istituzionale di politica scolastica l'implementazione di uno sportello d'ascolto, dove coloro che sentono il bisogno di un appoggio adulto possono fruire di una relazione comunicativa con gli psicologi che ha, come elemento fondante, l'ascolto scevro da giudizio alcuno.

INTERVENTI LIVELLO CLASSE:(Prevenzione Selettiva e Indicata)

1) sistemica osservazione dei comportamenti a rischio

2) Potenziamento delle competenze emotive, sociali e relazionali attraverso percorsi curriculari e di educazione socio-affettiva attraverso specifici interventi basati sulla Peer e Dispeer Education.

3) Utilizzo di stimoli culturali (narrativa, film, letture, rappresentazioni teatrali).

RUOLI E RESPONSABILITA':

IL DIRIGENTE SCOLASTICO:

- individua attraverso il collegio dei docenti un REFERENTE CYBERBULLISMO
- coinvolge tutte le componenti della comunita' scolastica nella prevenzione e nel contrasto al fenomeno, favorendo un utilizzo sicuro di internet a scuola

- promuove azioni di sensibilizzazione e prevenzione del fenomeno favorendo reti di intervento con enti, associazioni locali, altre scuoleprevede, all'interno del PTOF, corsi di aggiornamenti e formazione in materia di prevenzione dei fenomeni di bullismo e cyberbullismo, rivolti al personale docente ed Ata;
- favorisce la discussione all'interno della scuola, attraverso i vari organi collegiali, creando i presupposti di regole condivise di comportamento per il contrasto e la prevenzione dei fenomeni del bullismo e cyberbullismo;
- prevede azioni culturali ed educative rivolte agli studenti, per acquisire le competenze necessarie all'esercizio di una cittadinanza digitale consapevole.

IL REFERENTE DEL BULLISMO E DEL CYBERBULLISMO E TEAM EMERGENZA :

- promuovono la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale;
- organizzano attività di prevenzione ed informazione sulle sanzioni previste e sulle responsabilità di natura civile e penale, anche con eventuale affiancamento di genitori e studenti;
- intervengono in casi verificati rispettando il protocollo d'Istituto;
- coinvolgono partner esterni alla scuola, quali servizi sociali e sanitari, aziende del privato sociale, forze di polizia, per realizzare un progetto di prevenzione;
- curano rapporti di rete fra scuole per eventuali convegni/seminari/corsi e per la giornata mondiale sulla Sicurezza in Internet, la "Safer Internet Day" (SID);
- promuovono la dotazione del proprio istituto di una e-Policy, con il supporto di "Generazioni Connesse".

I DOCENTI:

- intraprendono azioni congruenti con l'utenza del proprio ordine di scuola, tenuto conto che l'istruzione ha un ruolo fondamentale sia nell'acquisizione e rispetto delle norme relative alla convivenza civile, sia nella trasmissione dei valori legati ad un uso responsabile di internet;
- valorizzano, nell'attività didattica, modalità di lavoro di tipo cooperativo e spazi di riflessioni adeguati al livello di età degli alunni;
- monitorano atteggiamenti considerati sospetti o preoccupanti degli alunni, dandone immediata comunicazione al Dirigente Scolastico;
- si impegnano a rimanere aggiornati sulle tematiche del cyberbullismo, anche attraverso corsi di aggiornamento proposti dalla scuola.

I GENITORI:

- partecipano attivamente alle azioni di formazione/informazione, istituite dalle scuole, sui comportamenti sintomatici del bullismo e del cyberbullismo
- conoscono il Regolamento disciplinare d'Istituto;

GLI ALUNNI:

- conoscono il Regolamento disciplinare d'Istituto

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).

Gli atti di cyberbullismo possono essere suddivisi in due gruppi:

- diretto: il bullo utilizza strumenti di messaggistica istantanea come SMS o MMS, che hanno un effetto immediato sulla vittima poiché diretti esclusivamente alla persona;
- indiretto: il bullo fa uso di spazi pubblici della Rete, come Social network, blog o forum, perdiffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima, anche dal punto di vista psicologico.

Indicatori di segnali che può manifestare una potenziale vittima di cyberbullismo sono:

- Appare nervosa quando riceve un messaggio o una notifica;
- Sembra a disagio nell'andare a scuola o finge di essere malata (ha spesso mal di stomaco o mal di testa);
- Cambia comportamento ed atteggiamento in modo repentino;
- Mostra ritrosia nel dare informazioni su ciò che fa online;
- Soprattutto dopo essere stata online, mostra rabbia o si sente depressa;
- Inizia ad utilizzare sempre meno PC e telefono (arrivando ad evitarli);
- Perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;
- Il suo rendimento scolastico peggiora.

Finalità condivisa tra scuola e famiglia è intervenire preventivamente ed efficacemente, al fine di evitare, arginare ed eliminare possibili manifestazioni di comportamenti antisociali. Valutare i comportamenti che sfociano in disagio sociale è precursore di un lavoro in rete, con la possibilità di coinvolgere anche un servizio specialistico socio-sanitario (Psicologo della scuola, Consultorio familiare, Servizi di Neuropsichiatria, etc.), quale supporto e/o forme di mediazione.

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.

La scuola prevederà per i docenti

- Formazione sul fenomeno dell'odio online per fornire loro strumenti di analisi e strumenti operativi per riconoscere, prevenire e combattere l'odio, online e offline., ma anche sulla conoscenza del linguaggio e su un uso responsabile per gli alunni:
- Progetti di educazione al dibattito ed all'argomentazione
- Progetti per la promozione delle pari opportunità ed il contrasto degli stereotipi di genere

---

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?

L'istituto , attraverso l'uso di una didattica attiva, che coinvolga docenti, studenti e famiglie, si propone di fare formazione e di indicare strategie per un uso più consapevole delle tecnologie nell'ottica della educazione alla Cittadinanza Digitale .

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.

La Legge 19 luglio 2019 n. 69, all’articolo 10, ha introdotto in Italia il reato di "revenge porn", ossia la diffusione illecita di immagini o di video sessualmente espliciti.
I rischi del sexting, legati al revenge porn, possono contemplare: violenza psico-sessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell’altro e depressione.

4.6 - Adescamento online

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

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

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

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

All'interno dell'Istituto oltre ai docenti curricolari e il responsabile di plesso, vi è un referente di bullismo e cyberbullismo e uno psicologo scolastico (Sportello di Ascolto), con il compito di accogliere/supportare gli studenti e le studentesse che non saranno

giudicati, ma compresi ed ascoltati.

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.

E' necessaria una attività di prevenzione che porti i più giovani ad acquisire competenze in grado di orientarli e guidarli nelle loro scelte online; ecco perché è fondamentale un'attività di educazione all'affettività e alle relazioni.

Il nostro piano d'azioni

AZIONI da sviluppare nell'arco del triennio 2021-2024

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un -utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse, anche con l'ausilio di esperti (iniziativa "Cuori Connessi").
- Organizzare percorsi formativi sui rischi associati all'uso della rete per i docenti.
- Organizzare uno o più incontri formativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori con il coinvolgimento di esperti.
- Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrati nello svolgimento della didattica per studenti/studentesse
- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- 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.

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

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

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

segnalare la presenza di materiale pedopornografico online.

Il personale docente deve porsi come "osservatore" delle dinamiche sociali e relazionali presenti all'interno dei gruppi classe con particolare attenzione ai segnali di problematiche legate ai rischi della rete. Inoltre ogni docente deve essere pronto e disponibile a recepire segnalazioni o sospetti, provenienti dagli alunni o dalle famiglie.

Si intende incrementare la sezione del sito dell'Istituto dedicata alle problematiche in questione con suggerimenti ed indicazioni per il riconoscimento delle problematiche piu' frequenti.

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.

Uno strumento utile per raccogliere informazioni può essere il diario di bordo (allegato alla presente e-Policy): il docente deve cercare di capire se gli episodi sono circoscritti al gruppo o se interessano l'intero Istituto. Operativamente è fondamentale coinvolgere tutti gli studenti e le studentesse, informandoli sui fenomeni e sulle caratteristiche degli stessi, suggerendo di chiedere aiuto se pensano di vivere situazioni, di subire atti identificabili come bullismo o cyberbullismo.

5.3. - Gli attori sul territorio

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

Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

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

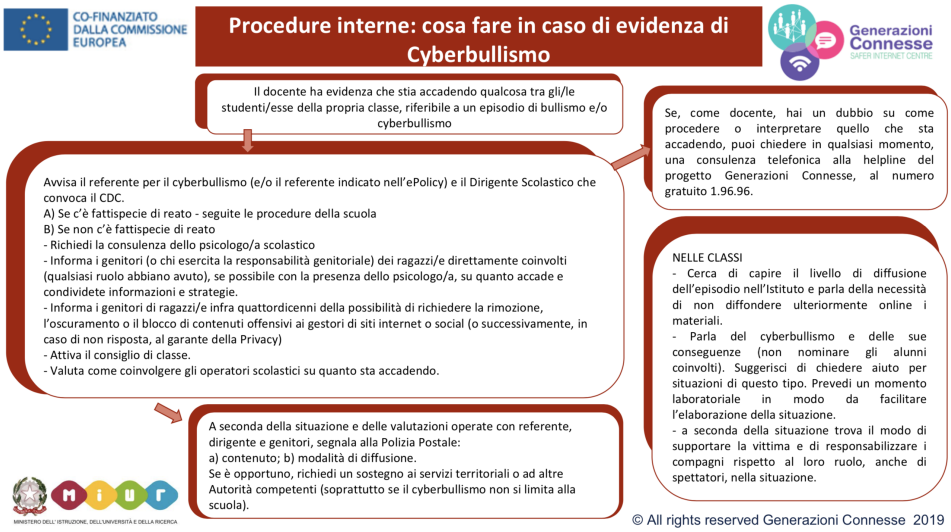
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di

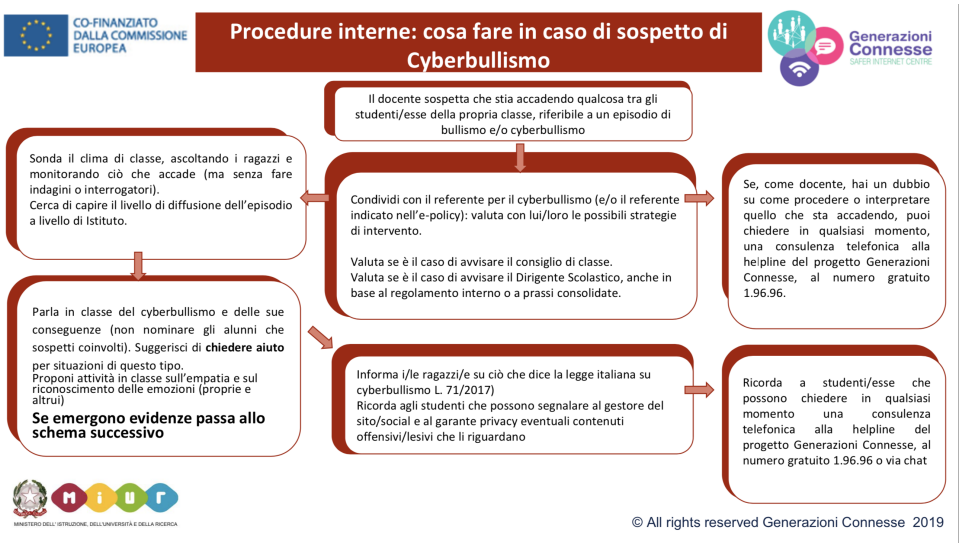
governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.

- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni**: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico**: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

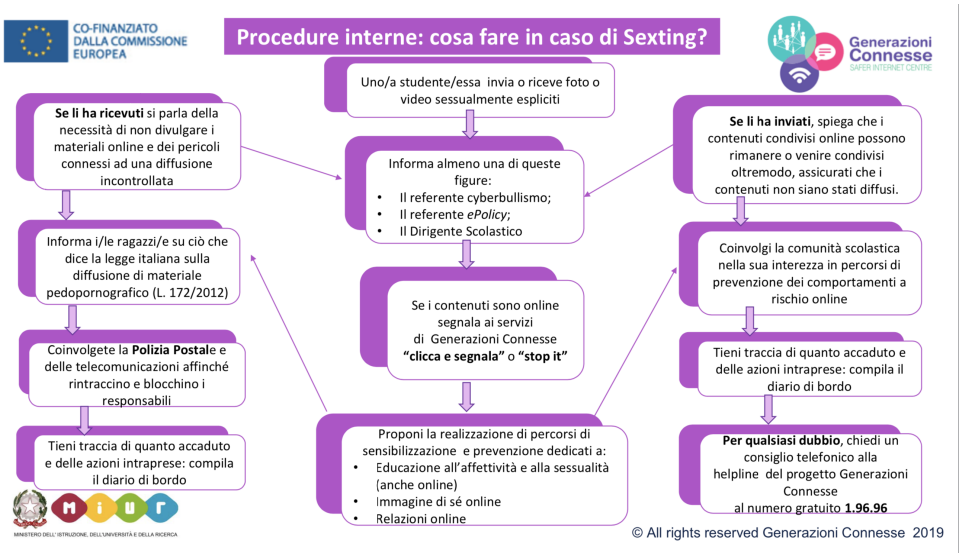
5.4. - Allegati con le procedure

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

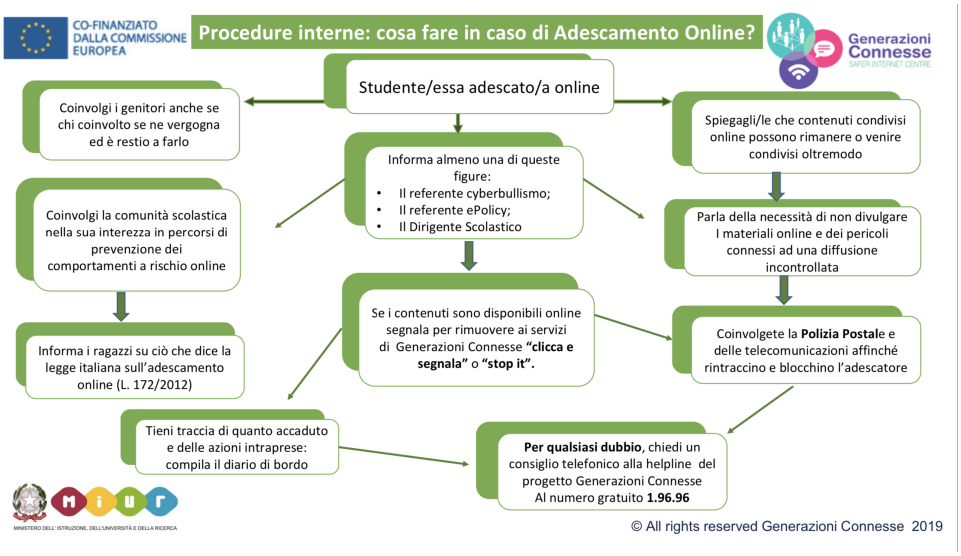




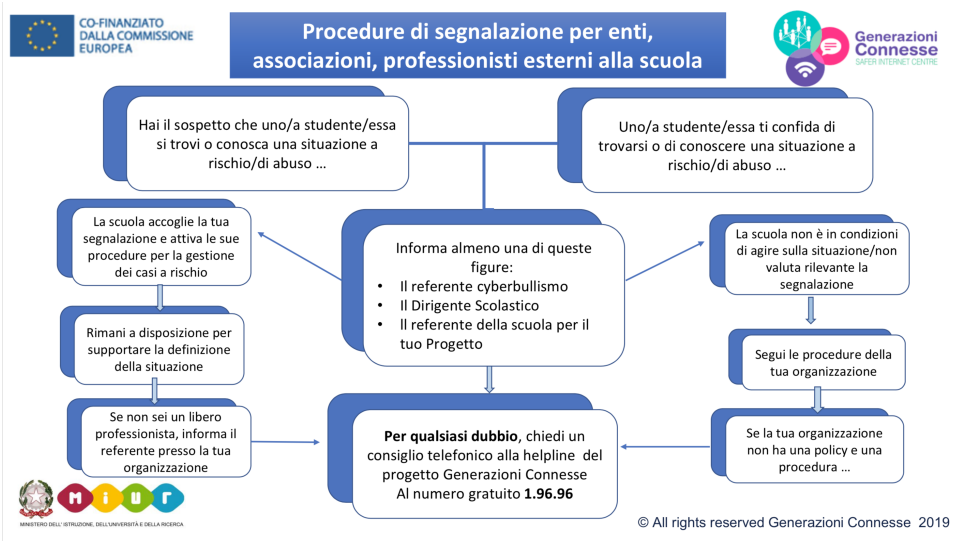
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Il nostro piano d'azioni

L'Istituto si pone l'obiettivo di una collaborazione sinergica tra scuola-famiglia-servizi territoriali, al fine di creare azioni condivise nell'ottica della prevenzione e protezione della comunità scolastica dai rischi legati da un uso scorretto del Digitale.