Documento di ePolicy

NAMM488001

S.G.BOSCO-SUMMA VILLA-S0MMA VES

PIAZZA VITTORIO EMANUELE III - 80049 - SOMMA VESUVIANA - NAPOLI (NA)

Dirigente Scolastico Prof. ssa Liguoro Rosa

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.

In particolare il nostro Istituto attraverso l'E-policy si propone di definire sia le norme comportamentali di utilizzo delle TIC, in particolare delle apparecchiture informatiche collegate alla rete in dotazione alla Scuola, sia azioni formative ed educative per far acquisire agli alunni competenze " tecniche", ma anche corrette norme comportamentali per prevenire, rilevare e fronteggiare i rischi che derivano da un utilizzo non responsabile, pericoloso o dannoso delle tecnologie digitali. Il documento potrà essere revisionato annualmente.

1.2 - Ruoli e responsabilità

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

Il Dirigente scolastico

- E' responsabile per la sicurezza dei dati
- E 'informato sulle linee guida contenute nella E-policy ed é garante della sua applicazione
- Provvede periodicamente alla revisione della E-policy, in collaborazione con l'Animatore Digitale, il Collegio dei Docenti e il Consiglio d'Istituto anche in funzione dell'evoluzione delle tecnologie digitali
- Garantisce l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza online
- Supporta i docenti nelle procedure per la segnalazione e gestione dei casi che dovessero verificarsi

L'Animatore Digitale

- Collabora alla revisione e all'aggiornamento della E-policy e diffonde i suoi contenuti alla comunità scolastica con la pubblicazione della stessa sul sito web della scuola
- Favorisce la formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale e della sicurezza in rete" e fornisce consulenza e informazioni al personale, in relazione ai rischi online e alle misure di prevenzione e di

gestione degli stessi
- Coinvolge la comunità scolastica nella partecipazione ad attività e progetti attinenti "la scuola digitale"e individua i fabbisogni dell'Istituto proponendo soluzioni metodologiche e tecnologiche innovative e sostenibili

Il Referente del Bullismo e Cyberbullismo

- Aggiorna la E-policy in collaborazione con tutti i soggetti interessati e con l'Animatore Digitale
- Promuove progetti, attività, eventi, informa e indirizza la comunità scolastica sulle problematiche inerenti al billismo e al cyberbullismo

I docenti

- Devono informarsi e aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di Internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento
- Inseriscono nella didattica tematiche attinenti alla siciurezza online e trattano le problematiche della comunicazione multimediale
- Garantiscono che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effetuate con sistemi scolastici ufficiali
- Controllano l'uso delle tecnologie digitali da parte degli alunni durante le lezioni e ogni altra attività didattica (ove é consentito) e nelle lezioni in cui é programmato l'utilizzo di Internet
- Guidano gli alunni a siti controllati e li verificano come adatti per il loro uso e controllano che nelle ricerche su Internet siano trovati e trattati solo materiali donei
- Prevengono e intercettano situazioni legate ad un 'uso scorretto delle nuove tecnologie e ai rischi di rete

I genitori

- Sostengono la scuola nel promuovere la sicurezza online, conoscendo l'E-policy, i Regolamenti dell'stituto e partecipano agli incontri organizzati dalla scuola sui temi della sicurezza online
- Collaborano con la scuola per l'utizzo corretto delle TIC nella didattica e monitorano l'uso che fanno i figli di Internet a casa
- Prevengono e intercettano situazioni legate ad un uso scorretto delle nuove tecnologie da parte di singoli alunni o in gruppo e le seganalano alla scuola
- Vigilano sui device dei propri figli al fine di prevenire e intercettare situazione a rischio

Gli alunni

- Conoscono e rispettano la E-policy e i Regolamenti (generali e specifici sul cyberbullismo)

- Segnalano al docente din classe eventuali usi impropri della rete e dei dispositivi da parte dei compagni
- Conoscono le buone pratiche di sicurezza online e adottano condotte rispettose degli altri anche qundo si comunica in rete
- Costruiscono una cittadinaza digitale comprendendo le potenzialità offerte dalle TIC

Il personale ATA

- Collabora nella prevenzione ed intercettazione di situazioni legate ad un uso scorretto della E-policy

---

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).

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.

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

Il presente documento di E-policy verrà pubblicato sul sito istituzionale della scuola nella sezione Regolamenti.

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 violazioni delle norme previste dalla E-policy comportano l'irrogazione di sanzioni disciplinari secondo quanto previsto dal Regolamento d'Istituto, dal Regolamento per il contrasto al Bullismo e al Cyberbulismo e dal Patto di Corresponsabiltà. Nei casi più gravi potrebbero anche configurarsi reati perseguibili d'ufficio o a querela di parte, come previsto dai riferimenti normativi e da specifica norma n.71 del 29 aggio 2017.

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 si integra con gli obiettivi del PTOF, con il Regolamento d'Istituto, con il Regolameto per il contrasto al bullismo e al cyberbullismo, con il Regolamento per l'utilizzo del Laboratorio informatico e con la normativa vigente.

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 l'implementazione della E-policy e il suo aggiornamento sarà svolto dal Dirigente Scolastico con la collaborazione dell'Animatore Digitale e del TID, del Referente del bullismo e cyberbullismo, sulla base delle segnalazioni effettuate e delle esigenze dell'Istituto.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

Diffondere la conoscenza del progetto Generazioni connesse e informare i docenti, i genitori e gli alunni sulle tematiche del progetto attraverso i materiali disponibili sul sito www.generazioniconnesse.it

Azioni da svolgere nei prossimi 3 anni:

Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'E-policy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.

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.

Competenza digitale significa padroneggiare certamente le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con "autonomia e responsabilità" nel rispetto degli altri e sapendone prevenire ed evitare i pericoli. Ne deriva che tutti gli insegnamenti sono coinvolti nella sua costruzione. Educare alla cittadinanza digitale é progettare esperienze di apprendimento in cui tutti gli allevi sino chiamati ad agire tutte le competenze integrando la dimensione analogica e quella digitale.In virtù della valenza trasversale della competenza digitale, la loro acquisizione verrà promossa **attraverso attività progettuali d'Istituto e percorsi didattici disciplinari e/o interdisciplinari.**L'eventuale progettazione di unità didattiche particolari potrà essere oggetto di pianificazione a livello di Dipartimenti disciplinari, e comunque andrà calibrata sulle esigenze reali di ogni classe. Coerentemente con gli obiettivi individuati nel curricolo, **l'Istituto attiverà dei percorsi didattici finalizzati al conseguimento di una cittadinanza digitale degli alunni sulla base delle seguenti aree di competenza:**

-Sviluppo delle abilità di base nelle TIC

-Alfabetizzazione mediatica (conoscenza e funzioni dei principali mezzi di comunicazione)

-Comunicazione e collaborazione in rete (strategie di comunicazione, rispetto della netiquette, rispetto delle diversità)

-Creazione di contenuti digitali

-Uso critico delle fonti (selezione e affidabilità di fonti, dati e contenuti, ricoscimento delle fake news)

-Benessere psicofisico ed educazione all'affettività

-Problem solving

-Sicurezza:

- **Prevenzione e riconoscimento di abusi -dipendenze (cyberbullismo-gioco d'azzardo ecc)**
- **Privacy e protezione dei dati personali e della propria identità digitale**
- **Netiquette e linguaggio della comunicazione online**

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

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

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

L'istituto, in coerenza con quanto affermato nel P.T.O.F., incrementa la formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica attraverso le seguenti azioni:

-Individuazione e formazione di un Animatore Digitale che accompagna il Dirigente Scolastico e il DSGA nell'attuazione degli obiettivi e delle innovazioni previste dal PNSD

- Supporto da parte di un Team per l'innovazione digitale per la promozione della didattica multimediale

-Iscrizione del Referente del Cyberbullismo alla Piattaforma ELISA (Formazione in E-Learning degli Insegnanti sulle Strategie Antibullismo)

-Raccolta del materiale fornito dal progetto Elisa in una banca dati accessibile a tutto il corpo docente

-Partecipazione al progetto Generazioni connesse e agli eventi indicati in relazione al Safer Internet (es. Safer internet day)

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

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

L'Istituto si impegna a favorire la formazione del personale docente con:

- Corsi di formazione e aggiornamento interni e esterni all'Istituto su programmi e software specifici relativi alle singole discipline e/o volti all'acquisizione di competenze digitali trasversali

-Autoformazione e formazione a distanza

-Partecipazione a incontri e corsi con esperti esterni

2.4. - Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

La scuola avrà cura di sensibilizzare le famiglie sull'utilizzo consapevole delle TIC e della rete con particolare attenzione alle situazioni di rischio on-line attraverso:

-Incontri con esperti ad un corretto uso delle nuove tecnologie da parte dei ragazzi a casa e a scuola, indicando anche alcune semplici azioni che possono rendere la navigazione sicura

-Presentazione sul sito web del portale www.generazioniconnesse.it e l'invito a consultarlo da parte di genitori

- L'inserimento nel Patto di Corresponsabilità di un riferimento all'utilizzo consapevole delle TIC e della Rete

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020)

Analizzare il bisogno formativo del corpo docente sull'utizzo consapevole e sicuro di Internet e delle tecnologie digitali

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

AZIONI (da sviluppare nell'arco dei tre anni scolastici

successivi)

Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilzzo e integrazione dell TIC nella didattica

Integrare l'utilizzo delle TIC nell'offerta didattica generale in maniera pianificata e strutturata

Promuovere la partecipzione del corpo docente a corsi gratuiti in modalità e-learning

Promuoverela partecipazione del corpo docente a corsi di formazione sull'utilizzo e l'integrazione delle TIC nella didattica e sull'uso consapevole delle tecnologie e di Internet

Creare un gruppo di lavoro interdisciplinare per valorizzare e ottimizzare le competenze

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.

Si ricorda a tutto il personale scolastico che il segreto professionale o d'ufficio obbliga a non rivelare le informazioni aventi natura di segreto, secondo un codice etico (legato al rispetto della persona), deontologico (come norma di comportamento professionale) e giuridico. È conseguentemente vietato al personale scolastico di divulgare personalmente o di pubblicare su blog, social network o siti personali qualunque informazione possa violare il segreto d'ufficio. Ogni docente è responsabile del proprio username e della propria password di accesso al registro elettronico. In caso di smarrimento o dimenticanza i docenti o il personale ATA possono 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. Il personale scolastico, nello svolgimento delle proprie mansioni, deve prestare particolare attenzione a:

- Non divulgare ad estranei le informazioni di cui viene a conoscenza durante il servizio
- Non fare copie, per uso personale, dei dati sensibili
- Osservare i criteri di riservatezza
- Trattare i dati in modo lecito e secondo correttezza
- Trattare i dati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati
- Comportarsi nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione, di perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta

---

3.2 - Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi*

presupposti sostanziali e non solo come possibilità di collegamento alla Rete.

4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

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

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

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

L'accesso a Internet è possibile e consentito per la didattica in tutti Plessi della scuola attraverso reti LAN e WiFi. I computer portatili collocati nelle aule accedono ad Internet attraverso rete WiFi.
Tutti i computer presenti nella scuola hanno installato un antivirus. Gli studenti non possono accedere con i loro dispositivi personali alla rete internet della scuola.I docenti possono accedere con i loro dispositivi personali alla rete solo per scopi didattici.
Gli studenti possono accedere ad Internet solo in occasione di attività didattiche .
L''accesso alla rete è comune per ogni plesso e permette tramite rete LAN o Wifi (attraverso l'impostazione di una password) di accedere al web per esigenze didattiche e per redigere giornalmente il registro elettronico.
I computer portatili presenti nelle aule non richiedono una password di accesso per l'accensione e hanno filtri per la navigazione quindi ogni docente è quindi tenuto ad un controllo da parte dell'uso degli alunni della strumentazione.

3.3 - Strumenti di comunicazione online

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

e-Mail

La scuola è dotata di un account di posta elettronica che é utilizzato ordinariamente dagli uffici per l'invio della documentazione di servizio. La nostra scuola usufruisce dei servizi Google e gestisce un proprio spazio. Ogni docente possiede un account Google Suite for education.L'account è strettamente personale, per cui ogni utente dovrà avere cura di disconnettere il proprio accesso al termine del suo utilizzo. Lo spazio è destinato alla ricezione di comunicazioni, all'invio di documentazione e alla condivisione di materiali con altri docenti e con gli alunni. Sono stati creati degli account anche per gli studenti, per i quali però è solo attivo il servizio drive, poiché l'uso è esclusivamente didattico.

Sito web della scuola

La scuola attualmente ha un sito web aggiornato ww.smsangiovannibosco.edu.it, in cui sono pubblicati i contenuti delle proposte formative e del settore didattico, nonché le circolari, gli avvisi e lecomunicazioni.Il sito web della scuola è gestito dal team digitale ed é possibile accedere all'area riservata del sito con una password.

Social network

La scuola ha approvato il Regolamento della pagina istituzionale Instagram per la creazione di un'apposita pagina istituzionale sul social suddetto.

Registro elettronico

Il Registro elettronico Nuvola è uno strumento al quale possono accedere tutti i membri della comunità scolastica, previa registrazione da parte della segreteria. Tutti gli utenti devono essere provvisti di nome utente e password. L'uso del registro é personale e riservato: ogni utente deve provvedere affinché i dati di login restino riservati e si impegna a cambiare password nel caso in cui la riservatezza degli stessi sia stata violata.

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.

Alunni

Gli alunni non posso utilizzare i cellulari personali a scuola. In casi particolari espressamente autorizzati dal Dirigente scolastico è possibile portare a scuola il cellulare ma spento e nello zaino. .Per questi alunni si provvederà a stilare un elenco che verrà allegato al Registro di classe. In caso di uscite didattiche, viaggi d'istruzione, recite, progetti sul territorio ed altre situazioni affini gli alunni potranno usare dispositivi personali ma rispettando le regole di utilizzo. Le foto e i video eventualmente registrati in queste occasioni, dietro autorizzazione dei docenti, dovranno avere un uso personale e non potranno essere diffusi in rete qualora siano state riprese terze persone (altri alunni, genitori, docenti ed operatori). L'Istituto non sarà ritenuto responsabile in caso di furto o danneggiamento accidentale

I Docenti

I docenti possono utilizzare i dispositivi della scuola per realizzare tutte le attività connesse alla funzione docente. E' consentito per i docenti l'uso dei propri dispositivi in classe per quanto attiene l'attività didattica qualora siano necessari, ma non possono essere utilizzati durante le lezioni per questioni personali. È consentito l'uso

di strumentazioni personali (notebook, tablet…) per attività didattiche o extracurricolari, ma l'Istituto non sarà ritenuto responsabile in caso di furto o danneggiamento accidentale. Non è, comunque, consentito l'acceso ad internet attraverso la rete scolastica per fini personali.

Altri operatori

Tutti gli altri operatori presenti a qualsiasi titolo nella scuola (esperti esterni, collaboratori, ditte esterne...) dovranno attenersi alle norme previste per il personale scolastico.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020)

Organizzare incontri formativi rivolti a genitori e alunni sui rischi del web

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

Dotare la scuola di filtri di sicurezza per la navigazione in internet

Realizzare azioni inerenti al PNSD

Organizzare un sistema di raccolta , in modalità anonima, delle questioni considerate rilevanti per gli alunni e i docenti di cui la scuola si dovrebbe occupare

Informare gli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali , dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

Coinvolgere gli studenti nella produzione di contenuti per il sitp web e la pagina istituzionale Instagram

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.*

La prevenzione è lo strumento più efficace per proteggere i minori dai pericoli online. Lo strumento principale della prevenzione é l'informazione che si articola attraverso le misure e le iniziative che l'Istituto pone in essere attraverso le figure di sistema ovvero l'Animatore Digitale, il Referente del Bullismo e Ciberbullismo, il Referente per la legalità e i docenti del team digitale (incontri formativi con esperti, percorsi curricolari

e extracuricolari, progetti, accordi di rete ecc) per diffondere la conoscenza delle problematiche legate a un uso scorretto delle TIC e quindi per prevenirle, riducendo così il rischio di comportamenti problematici. Anche i genitori hanno un ruolo determinante in qualità di interlocutori di fiducia,pronti a intervenire attivamente se necessario. Difatti la prevenzione ha un approccio sistemico e coinvolge tutta la comunità scolastica attraverso un'azione di sensibilizzazione e di informazione.

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).

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.

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?

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.

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.

4.7 - Pedopornografia

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

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

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

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

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

impreviste del sexting.

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

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

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020)

Incontri formativi rivolti a genitori e studenti con il Comparto della Polizia Postale di Napoli sul fenomeno del cyberbullismo e i rischi del web

Informare, sensibilizzare e fornire informazioni e documenti ai docenti e alunni sui rischi del web

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

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

Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online nella scuola, educazione all'affettività- diversità e inclusione

Creare protocolli con gli Enti del territorio

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.

E' opportuno sottolineare che la rilevazione dei casi è compito dell'intera comunità educante e la collaborazione scuola-famiglia è di vitale importanza.Glli insegnanti, i genitori, il personale ATA, quando hanno il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di rischio cyberbullismo, sexting violazione della privacy, accesso a contenuti non adeguati lo **segnaleranno al docente Referente del bullismo e del cyberbullismo che provvederà a informare il Dirigente scolastico e il gruppo di lavoro preposto in base a procedure definite e stabilite nel "Protocollo per la gestione dei casi " del Regolamento per il contrasto al bullismo e al cyberbullismo del nostro Istituto.**

Le procedure illustrate in seguito per la seganlazione e gestione dei casi sono offerte dal progetto a titolo esemplificativo e/o informativo.

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.

L'Istituto dispone di una procedura di rilevamento e monitoraggio delle problematiche online che coinvolgono gli/le studenti/studentesse segnalati dai docenti al referente per il cyberbullismo e alla Dirigenza Scolastica e alle autorità locali (quando richiesto). I genitori coinvolti sono sempre informati. L'Istituto collabora attivamente con altre agenzie/istituzioni del territorio, per monitorare e migliore la gestione di tali episodi e gestire al meglio ed elaborare strategie di prevenzione. Per tutti i casi si segnalazione riferirsi al **Protocollo per la gestione dei casi " del Regolamento per il contrasto al bullismo e al 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.

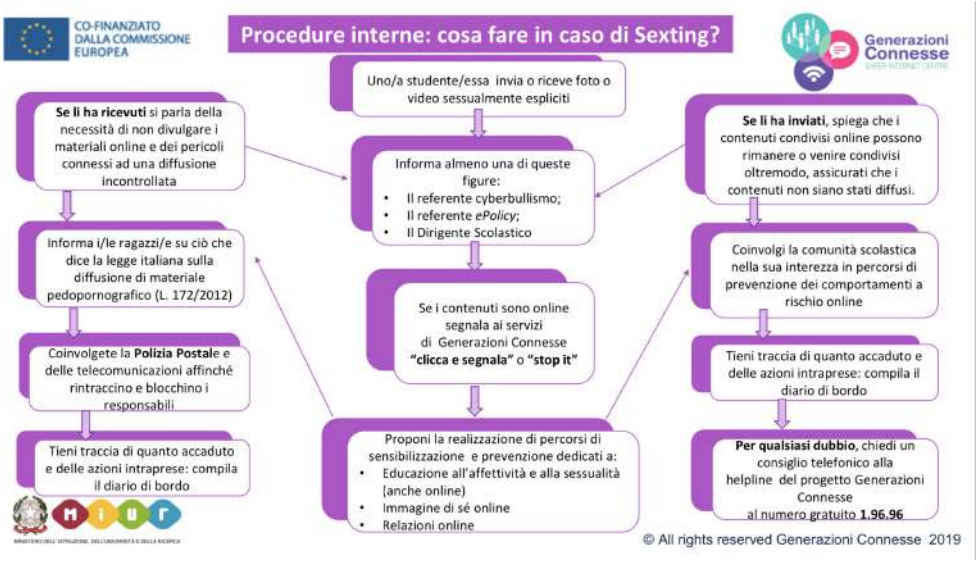
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **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.

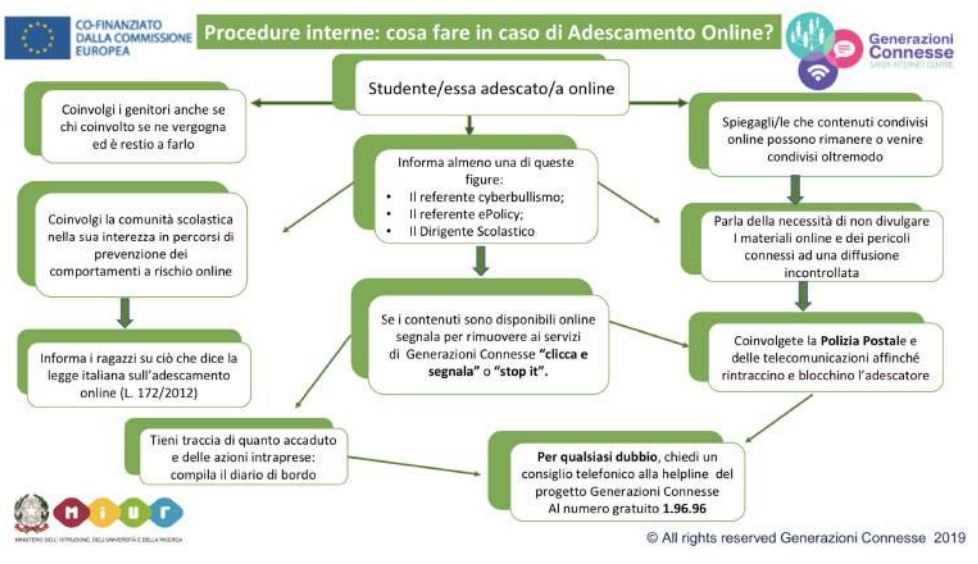
5.4. - Allegati con le procedure

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

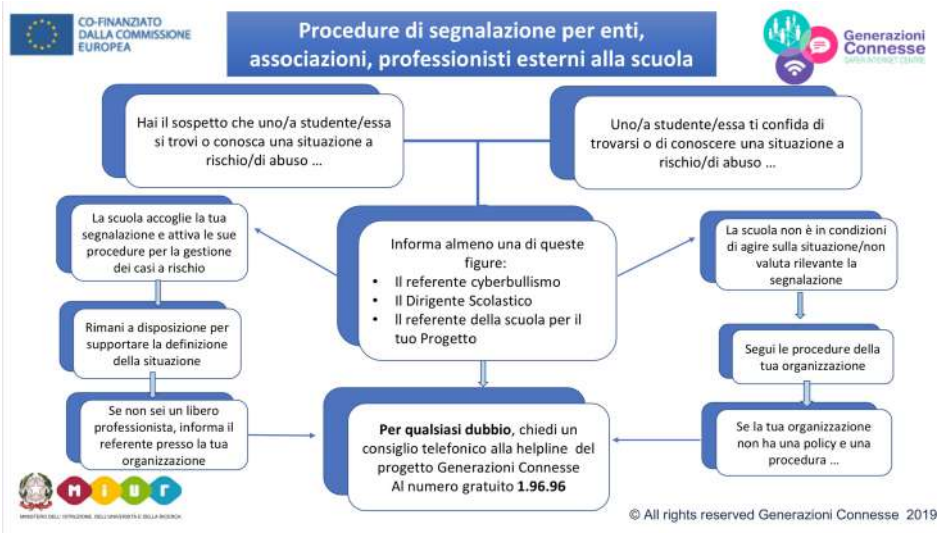
Procedure interne: cosa fare in caso di sexting?



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

Per le procedure sulla segnalazione delle situazioni a rischio riferirsi al "Protocollo per la gestione dei casi " del Regolamento per il contrasto al bullismo e al cyberbullismo del nostro Istituto.

Il nostro piano d'azioni

Scheda di segnalazione dei casi

Cassette del silenzio per le segnalazioni anonime

Assicurare, attraverso azioni specifiche, la conoscenza e la comprensione, da parte del corpo docente e del personale scolastico, delle procedure di rilevazione, monitoraggio e gestione dei casi di abuso o di altre problematiche associate all'utilizzo di Internet e delle tecnologie digitali.