Documento di ePolicy (revisione ottobre 2020)

NAIC8CY00B

NA - I.C. 41 CONSOLE

VIA DIOMEDE CARAFA 28 - 80124 - NAPOLI - NAPOLI (NA)

Dirigente Scolastico Maria Patrizia Di Marco

Argomenti del Documento

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.

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.

Il nostro **Istituto**, elabora questo documento seguendo le indicazioni delle LINEE di ORIENTAMENTO per azioni di prevenzione e di contrasto al bullismo e cyberbullismo elaborate dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con "Generazioni Connesse" e il Safer Internet Center per l'Italia, programma comunitario istituito dal DF C Europeo e dal Consiglio dell'Unione.
Lo scopo è quello di educare e sensibilizzare gli adolescenti, gli insegnanti e i genitori all'uso sicuro e consapevole di internet.
Pertanto, il nostro Istituto propone agli studenti e agli insegnanti di utilizzare internet per promuovere la crescita del curriculo scolastico di ciascun alunno attraverso la condivisione delle numerose risorse, l'innovazione e la comunicazione.
Di conseguenza i nostri insegnanti hanno l' onere di guidare gli studenti nelle attività on-line, di stabilire obiettivi chiari per un uso responsabile di internet. L'obiettivo principale resta quello di arricchire le attività didattiche, secondo quanto prevede il curricolo scolastico, l'età e la maturità degli studenti.
Per questo motivo, il nostro Istituto continua ad aderire al progetto **GENERAZIONI CONNESSE** , promosso dal MIUR in collaborazione con la comunità Europea. Il progetto è rivolto alle classi quarte, quinte della scuola primaria e tutte le classi della scuola secondaria di primo grado.
Nell'ambito di questo progetto l'istituto continua ad impegnarsi alla rimodulazione e alla stesura del documento Policy e-Safety già esistente, per disciplinare l'utilizzo delle Nuove tecnologie all'interno dell'Istituto e prevenire i rischi legati ad un utilizzo non corretto di internet.
Il documento di e-Safety Policy è volto a descrivere: il quadro del fenomeno, le regole comportamentali, i criteri per l'utilizzo delle TIC in ambiente scolastico, la gestione delle

problematiche connesse ad un uso non consapevole delle tecnologie digitali e la regolamentazione della nuova didattica utilizzata nel periodo lockdown "Covid-19"
Gli alunni devono essere interamente consapevoli dei pericoli occulti a cui si espongono quando navigano in rete. L'Istituto promuove l'adozione di metodi che limitino l'accesso a siti e/o applicazioni illeciti e invita gli insegnanti a guidare gli alunni nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose.

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

È responsabile della presentazione, di questo documento all'attenzione del Consiglio di Istituto e al Collegio dei Docenti. Deve anche valutare l'efficacia della politica e monitorarne/indirizzarne l'attuazione, anche in collaborazione con personale scolastico, enti locali, associazioni territoriali interessate, le autorità competenti e i servizi socio-sanitari del territorio per la gestione dei casi difficili. Al Dirigente spetta, inoltre, il compito di informare subito le famiglie dei minori coinvolti in atti di bullismo e cyberbullismo , se è necessario, convocare tutti gli interessati per adottare misure di assistenza alla vittima e percorsi rieducativi per l'alunno "provocatore".

Il Referente bullismo e cyberbullismo

"Ogni Istituto scolastico, nell'ambito della propria autonomia, individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo" (Art. 4 Legge n.71/2017, "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo" (permalink – file 1 LEGGE 71_2017 in allegato). Tale figura ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Fondamentale, dunque, il suo ruolo non solo in ambito scolastico ma anche in quello extrascolastico, in quanto (ove possibile) potrebbe coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.

Animatore digitale

Ha il compito di divulgare questo documento dentro la comunità scolastica in tutte le sue componenti (docenti/ata, genitori e studenti), mediante pubblicazione sul sito della scuola e cura la redazione e la revisione annuale della policy sulla base delle osservazioni ricevute da tutti i soggetti interessati. Si interessa inoltre, insieme al responsabile tecnico della scuola di contattare la ditta che gestisce l'assistenza tecnico-informatica per definire le misure di sicurezza informatica più opportune.

Personale docente, con particolare riferimento ai Coordinatori dei Consigli di Classe

Le insegnanti/gli insegnanti sono invitati a:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e aver letto, compreso e sottoscritto la presente policy;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'animatore digitale per

le opportune indagini / azioni / sanzioni;
- far comprendere e mettere in pratica alla componente studentesca le regole di comportamento relative alla sicurezza informatica;
- guidare la navigazione della componente studentesca, nelle lezioni in cui l'uso di Internet è pianificato, verso siti controllati come idonei per il loro uso, onde evitare di incontrare materiali inadatti.

Personale ATA

Il personale ATA è tenuto ad assicurare di:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica, la politica dell'Istituto, le relative buone pratiche e aver letto, compreso e sottoscritto la presente policy;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'animatore digitale per le opportune indagini / azioni / sanzioni;

Componente studentesca

Le alunne/gli alunni devono essere responsabilizzati sull'uso corretto dei sistemi informatici e della tecnologia digitale in accordo con i termini previsti da questa policy.
In particolare devono:

- conoscere il regolamento d'Istituto in riferimento all'uso dispositivi digitali personali
- avere una buona comprensione delle possibilità di ricerca sul web e della necessità di evitare il plagio, rispettare le normative sul diritto d'autore, non diffondere dati personali; comprendere l'importanza della segnalazione di ogni abuso, uso improprio o accesso a materiali inappropriati
- e conoscere il protocollo per tali segnalazioni;
- conoscere e comprendere le politiche sull'uso di dispositivi mobili;
- capire le politiche di utilizzo delle immagini ed essere consapevoli del significato e della gravità del cyber-bullismo.
- capire l'importanza di adottare buone pratiche di sicurezza informatica in tutti i momenti della vita, a tutela dell'incolumità propria e altrui e per evitare di perpetrare reati punibili sia a livello scolastico sia da parte della magistratura.

Genitori

Genitori e tutori svolgono un ruolo importante nel garantire che i loro figli comprendano la necessità di utilizzare i dispositivi Internet e mobili in modo corretto. La scuola ha il compito di informare le famiglie sull'approvazione della legge contro il Cyberbullismo in vigore dal 18 giugno 2017 e sull'esistenza di questo documento redatto sulle indicazioni di "Generazioni Connesse" e coglierà ogni occasione per sensibilizzare i genitori circa questi problemi attraverso circolari, sito web e altre comunicazioni telematiche, informazioni su campagne di sicurezza promosse da altre istituzioni o su convegni dedicati a questo tema. I genitori saranno incoraggiati a sostenere la scuola nel promuovere le buone pratiche di e-Safety e a seguire le linee guida sull'uso appropriato di:immagini digitali e video registrati in occasione di eventi scolastici, anche al di fuori delle aule;

- accesso alle sezioni del sito dedicate ai genitori, con particolare riguardo al registro elettronico;
- dispositivi personali dei loro figli durante i viaggi e le uscite didattiche.

Per un approfondimento sui ruoli e le responsabilità delle figure presenti a scuola: Legge 59/97, Art. 21 CO° 8; Legge N.165/2001 Art. 25; CCNL; DPR n. 275/99; Legge n.107/2015;
Piano Nazionale Scuola Digitale.
Vi ricordiamo, inoltre, che esiste una corresponsabilità educativa e formativa che riguarda sia i genitori che la scuola nel percorso di crescita degli studenti e delle studentesse.
Inoltre, rammentiamo che esiste una corresponsabilità educativa e formativa che riguarda sia i genitori che la scuola nel percorso di crescita degli studenti e delle studentesse; si può parlare di tre tipologie di " CULPA" :
culpa in vigilando: concerne la mancata sorveglianza attiva da parte del docente responsabile verso il minore (cosi come da art. 2048 del c.c.). Tale condizione è superabile se ci si avvale di una prova liberatoria di non aver potuto impedire il fatto (recita il terzo comma dell'art. 2048 c.c.: "le persone indicate nei commi precedenti sono liberate dalla responsabilità soltanto se provano di non aver potuto impedire il fatto").
culpa in organizzando: si riferisce ai provvedimenti previsti e presi dal Dirigente Scolastico ritenuti

come non soddisfacenti e quindi elemento favorevole al verificarsi dell'eventuale incidente.
culpa in educando: fa capo ai genitori i quali hanno instaurato una relazione educativa con il/la figlio/a, ritenuta come **non adeguata, insufficiente o comunque carente tale da metterlo/a nella situazione di poter recare danno a terzi.**

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).

Il nostro Istituto chiede a tutti gli attori esterni che in attivano per la realizzazione di attività educative, di conoscere e rispettare le regole che sono espicitate nel documento Poily e –Safety

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'Istituto si impegna ad attivare una serie di azioni e iniziative.
A partire **dalla pubblicazione sul sito della scuola** di questo documento aggiornato, si possono ipotizzare le seguenti azioni:
Per il corpo docente:

discussione collegiale sui contenuti, sulle pratiche indicate e su come inserire nel curricolo le tematiche di interesse della policy;

un confronto collegiale, su base annuale, circa la necessità di apportare modifiche e miglioramenti alla policy vigente;
elaborazione di protocolli condivisi di intervento.

Per gli alunni:

informative, depliant, materiale divulgativo, convegni con esperti esterni

Per i genitori:
l'organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare.

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.
Letta la **Legge 29 maggio 2017 n. 71** recante "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del Cyberbullismo" da oggi in vigore, il nostro Istituto regolamenta la gestione della policy in base alla gravità delle infrazioni messe in atto dal minore.
Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali di internet di cui si dispone per la didattica, in relazione alla fascia di età considerata, sono prevedibilmente le seguenti:

- un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;
- l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;
- la condivisione di immagini intime o inappropriate;
- la comunicazione incauta e senza permesso con sconosciuti;

Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo dell'alunno.
Infatti più gli alunni sono piccoli, più i comportamenti "da correggere" sono dovuti a uno sviluppo cognitivo e affettivo incompleto o a fasi critiche transitorie, che devono essere compresi e orientati proprio dagli educatori, nella prospettiva del raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno.
Sono previsti pertanto da parte dei docenti provvedimenti "disciplinari"proporzionati all'età e alla gravità del comportamento come riportati nel nostro vigente Regolamento d'Istituto.

1.6- INTEGRAZIONE dell'ePolicycon Regolamenti vigenti

Il nostro Istituto ha in dotazione strumenti tecnologici in seguito all'approvazione dei progetti didattici per favorire la formazione del personale e far crescere le competenze professionali specifiche nell'impiego delle nuove tecnologie.
A tal fine è stato stilato un Regolamento per l'utilizzo e il corretto funzionamento delle aule scolastiche, aule 2.0, delle LIM e delle postazioni informatiche, tramite l'indicazione di prassi opportune e l'invito ad un uso sempre più professionale da parte di tutto il personale.
Le apparecchiature presenti nel nostro Istituto sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto, minimizzando gli sprechi di risorse a disposizione (energia, carta, inchiostro, etc.). L'utilizzo delle apparecchiature è regolamentato da criteri che puntano a massimizzare la collaborazione collegiale: le prenotazioni, la tracciabilità delle apparecchiature, la segnalazione di malfunzionamenti, sono accorgimenti necessari per evitare disguidi organizzativi, smarrimenti, per rintracciare tramite i docenti la causa di un malfunzionamento, etc.

Gli insegnanti sono responsabili delle TIC nell'ambito dell'attività didattica e hanno il compito di responsabilizzare gli alunni per divenire consapevoli dell'importanza della salvaguardia di un bene comune, seguendo le corrette norme di utilizzo.
A tal fine, per garantire la sicurezza in rete sono state previste alcune strategie:

a. coinvolgimento dei genitori come partner educativi nei percorsi di formazione che riguardano gli studenti;

b. controllo (una tantum e/o all'evenienza di episodi dubbi) del sistema informatico (cronologia, cookies, ecc.) da parte dei responsabili;
c. installazione di firewall sull'accesso a Internet;
d. presenza di un docente o di un adulto responsabile durante l'utilizzo di Internet, della piattaforma o di altre TIC;
e. aggiornamento periodico del software antivirus e scansione delle macchine in caso di sospetta presenza di virus;
f. utilizzo di penne USB, CD/DVD o altri dispositivi esterni personali, solo se autorizzati;
g. avvio di laboratori dedicati alla Cittadinanza Digitale (progetto PON-FSE "Vai avantid di un pixel").
h. Inserimento nel PTOF triennale di 20 ore annuali di "informatica" per gli alunni delle classi III della scuola primaria fino alle classi II della scuola secondaria di I grado a cura dei docenti di Tecnologia.

1.7- Monitoraggio DELL'IMPLEMENTAZIONE della ePolicy e suo aggiornamento

Il documento della E-policy del Nostro Istituto, viene aggiornato periodicamente quando si presentano dei particolari cambiamenti, come è accaduto in questa seconda parte dell'anno scolastico 2019/2020. Infatti, il nostro Istituto durante il periodo di lockdown, ha cercato di attivarsi gradualmente ed efficacemente nella didattica a distanza favorendo una didattica inclusiva a vantaggio di ogni studente, utilizzando diversi strumenti di comunicazione, anche nei casi di difficoltà di accesso agli strumenti digitali e di sicurezza nella navigazione in rete.
Si è cercato di privilegiare un approccio didattico basato sugli aspetti relazionali della didattica e lo sviluppo dell'autonomia personale e del senso di responsabilità, orientato all'imparare ad imparare e allo spirito di collaborazione dello studente e in alcuni casi vedi l'infanzia, della collaborazione dei genitori. I nostri Docenti hanno dato la massima disponibilità del proprio tempo alle famiglie garantendo, anche attraverso l'uso di strumenti digitali e l'informazione sull'evoluzione del processo di apprendimento degli studenti e sullo sviluppo del senso di responsabilità digitale.

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.
Il nostro Istituto ha approvato, nell'anno scolastico 2018-19, il Curricolo verticale per le competenze digitali per tutti gli ordini di scuola. Il curricolo è pubblicato sul Sito web della scuola ed è parte integrante del PTOF.

2.2 - FORMAZIONE dei docenti SULL'UTILIZZO e L'INTEGRAZIONE delle TIC (Tecnologie DELL'INFORMAZIONE e della COMUNICAZIONE) nella didattica

Dall'anno dell'Istituzione dell 'I.C. 41 Console fino ad oggi, le risorse finanziarie destinate alla formazione dei docenti sono state utilizzate per :

- Informare la maggioranza dei docenti dei tre ordini di scuola sui contenuti e conseguenti azioni didattiche da intraprendere riferite alla Legge 170/2010 per la realizzazione di una scuola inclusiva.
- Informare la maggioranza dei docenti dei tre ordini di scuola sui contenuti e le TIC da usare nella didattica secondo il PNSD.
- Sollecitare i docenti a seguire i corsi di formazione proposti da Indire e altri corsi accreditati usando i fondi della carta del Docente (la scuola non ha fondi propri per la formazione).
- La formazione organizzata dell'Istituto con i fondi stanziati ad hoc per l'emergenz epidemiologica, sono stati usati per istruire i docenti sull'uso della piattaforma G-Suite (piattaforma condivisa per la didattica a distanza).

2.3 - FORMAZIONE dei docenti SULL'UTILIZZO consapevole e sicuro di Internet e delle tecnologie digitali

La nostra scuola ha già promosso momenti informtivi per i docenti sull' utilizzo delle TIC come metodologia di insegnamento-apprendimento, ma vuole impegnarsi in ulteriori occasioni di approfondimento sull' uso educativo delle tecnologie in rete con altre scuole ed altre realtà sociali presenti sul territorio. Verranno pertanto organizzati laboratori e/o eventi per sensibilizzare l' intera comunità scolastica (studenti, genitori, educatori) sui rischi della navigazione non controllata

2.4. - SENSIBILIZZAZIONE delle famiglie e INTEGRAZIONI al Patto di Corresponsabilità

La scuola ha il compito di informare le famiglie sull'approvazione della legge contro il Cybebullismo e sull'esistenza di questo documento redatto sulle indicazioni di "**Generazioni Connesse**" e coglierà ogni occasione per sensibilizzare i genitori circa questi problemi attraverso circolari, sito web e altre comunicazioni telematiche, informazioni su campagne di sicurezza promosse da altre istituzioni o su convegni dedicati a questo tema. I genitori saranno incoraggiati a sostenere la scuola nel promuovere le buone pratiche di e-Safety e a seguire le linee guida proposte anche nel Patto di corresponsabilità sull'uso appropriato di: immagini digitali e video registrati in occasione di eventi scolastici, anche al di fuori delle aule; accesso alle sezioni del sito dedicate ai genitori, con particolare riguardo al registro elettronico; uso dei dispositivi personali dei loro figli durante i viaggi e le uscite didattiche. Come già citato, il patto di corresponsabilità è stato integrato nell'a.s. 2019-20 con volantini informativi sull'uso responsabile di Internet; nel c.a.s. 2020-21 il patto, integrato per far fronte all'emergenza epidemiologica, ha sottolineato la "corresponsabilità" della scuola e dei genitori nell'educare gli alunni, impegnati nella DaD, all'uso consapevole dei device e di Internet per scipo didattici.

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

1. Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
2. Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
3. Adottare azioni idonee a colmare le carenze formative identificate dai risultati del monitoraggio.

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 personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.),nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Tutto il personale incaricato riceve poi istruzioni particolareggiate applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi.

Viene inoltre fornita ai genitori informativa e richiesta di autorizzazione file elaborati, se non quello operato dai docenti interessati sui supporti rimovibili personali.

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 nei laboratori multimediali sotto la vigilanza del docente accompagnatore. L'accesso è per tutti schermato da filtri free che dal server impediscono il collegamento diretto a siti appartenenti ad eventuali black list.
L'accesso al sistema informatico per la didattica, server e internet, nel laboratorio multimediale èconsentito a tutti.
L'accesso ad internet tramite i dispositivi mobili è consentito solo con una password.
I docenti registrano il proprio accesso, scrivendo su un registro la data e l'orario di utilizzo del laboratorio.
Non vi è un backup dei file elaborati, se non quello operato dai docenti interessati sui supporti rimovibili personali. Le postazioni del laboratorio funzionano come stazioni di lavoro e non come archivi.

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

L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. L'eventuale invio o ricevimento di posta ascopi didattici avverrebbe solo su autorizzazione del Dirigente Scolastico e operativamente sarebbesvolto dall'assistente amministrativo addetto. La posta elettronica è protetta da antivirus, e quellacertificata anche dall'antispam.

Sito web della scuola

La scuola attualmente ha un sito web istituzionale e un sito per una scuola inclusiva. Tutti i contenuti del settore didattico sono pubblicati direttamente e sotto supervisione di un docente esperto in siti Web e dell'Animatore digitale, che ne valuta con il Dirigente Scolastico la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc.

Social network

Attualmente nella didattica non si utilizzano social network, mentre l'istituzione scolastica ha creato una pagina di FACEBOOK col proprio profilo autorizzato dal Dirigente scolastico, dove vengono pubblicate le notizie sulle attività didattiche, come: viaggi, manifestazioni sportive, culturali e sociali.

3.4 - STRUMENTAZIONE personale

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

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

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

Per gli studenti

I telefoni cellulari, le relative fotocamere e registratori vocali non verranno utilizzati durante le lezioni scolastiche , mentre è concesso l'uso dei tablet all'interno di attività didattiche espressamente programmate dal corpo docente.
Si ricorda l'uso dei dispositivi mobili deve essere responsabilizzato, pertanto l''invio di materiali abusivi, offensivi o inappropriati è vietato, anche se avviene all'interno di cerchie o gruppi di discussione privati.
Gli alunni BES certificati, previa consultazione con il Consiglio di Classe, concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili.

Per il personale docente/ATA

Il personale docente ha il compito rispettare le norme presentate nel regolamento di Istituto e nella Policye – Safety durante l'uso della strumentazione fornita dalla scuola rispetto a quella personale (portatili, pc fissi, tablet …); le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali. Telefoni cellulari, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante l'orario di servizio, mentre l'uso del tablet è consentito all'interno di attività didattiche espressamente programmate.
La password di accesso alla rete wireless va custodita con cura e per nessuna ragione deve essere divulgata agli studenti.
Nel caso che si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale come chiavette usb, dischi fissi portatili è necessario controllare anticipatamente che essi siano liberi da virus per evitare di danneggiare le attrezzature comuni.
Durante l'attività didattica è conveniente che ogni insegnante:

- dia delle indicazioni sul corretto uso della rete (Internet, piattaforma studenti ecc.), condividendo con gli studenti le regole di comportamento di navigazione in rete;
- si assuma la responsabilità di segnalare prontamente eventuali malfunzionamenti o danneggiamenti al docente tecnico informatico;
- si assuma la responsabilità di cancellare nella cache della postazione informatica usata di classe qualsiasi account di accesso dove si evidenziano i dati personali, come l'accesso alla posta elettronica, al registro elettronico e ad eventuali piattaforme per l'apprendimento a distanza.

IL NOSTRO PIANO DI AZIONE NEL TRIENNIO

Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola e a casa da parte degli studenti e delle studentesse con particolare riguardo al periodo di attivazione della DaD o della DDI.
Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personalei ATA
Intraprendere azioni informative per il personale e gli alunni 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.*

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.

4.1 - 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 scolastico ha organizzato alcuni incontri di riflessione con gli alunni (della scuola secondaria) ed esperti esterni sulla tematica.

4.2 - 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.

4.3 - 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.

4.1 - 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'AZIONE PER IL TRIENNIO

Il nostro istituto Scolastico negli ultimi tre anni ha organizzato momenti informativi con alunni e genitori sulle tematiche del Cyberbullismo e in particolare un incontro con l'Associazione "Caramella Buona" sui temi della pedofilia. Il progetto finanziato dalla Regione Campania denominato " A scuola di Comunità" avrebbe dovuto trattare anche questa tematica ma, l'emergenza epidemiologica, ha bruscamente interrotto le attività . Si intende comunque, continuare su questa strada.

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.

Che cosa segnalare
Il personale della scuola deve essere attento alle rilevazione di un particolare comportamento in alcuni alunni; infatti, gli alunni che possono essere soggetti a forme di abuso psicologico, o fisico, o digitale dentro o
fuori dell'ambiente scolastico, mostrano segni di tristezza o di ansia o di insicurezza, o di rifiuto o di risentimento nei confronti di compagni o di altri; tale situazione determina una grossa difficoltà a comunicare il proprio stato d'animo.

Come segnalare: quali strumenti e a chi.
La scuola dopo aver rilevato un alunno in situazione di cyberbullismo deve assicurarsi che l'alunno vittima abbia tutta la sua attenzione nella ricerca di prove per accusare l'alunno o l'adulto colpevole.

Ricercare e conservare la prova è utile per far conoscere l'accaduto in base alla gravità ai genitori degli alunni, al Dirigente scolastico e per le condotte criminose alla polizia.
Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno, quantunque riferite a fatti accaduti dentro o al di fuori del contesto scolastico, la scuola ha il dovere di comunicare ai genitori e per fatti rilevanti anche al Dirigente scolastico; per quelle criminose, anche alla polizia.
In particolare la segnalazione viene fatta a entrambe le famiglie, se oltre alla vittima anche l'autore della condotta negativa è un altro alunno.
Per le segnalazioni di fatti rilevati sono previsti i seguenti strumenti che i docenti possono utilizzare sulla base della gravità dell'accaduto come riportati nel Regolamento d'Istituto Vigente,
Inoltre, per i reati meno gravi, la legge rimette ai genitori degli alunni la scelta di richiedere la punizione del colpevole attraverso la querela.
Per i reati più gravi (es. pedopornografia) gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti).
In particolare per i fatti criminosi, ai fini della denuncia,la relazione deve
essere redatta nel modo più accurato possibile, indicando i seguenti elementi: il fatto, il giorno dell'acquisizione del fatto nonché le fonti di prova già note e per quanto possibile, le generalità, il domicilio e quant'altro di utile a identificare la persona alla quale il reato è attribuito, la persona offesa, e tutti coloro che sono in grado di riferire circostanze rilevanti per la ricostruzione del fatto.

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.

Procedure operative per la gestione dei casi

CYBERBULLISMO: alcuni campanelli di allarme

Gli atti di bullismo avvengono prevalentemente entro o nei dintorni del contesto scolastico, tuttavia in misura crescente le prepotenze vengono riportate nel contesto virtuale di internet. In queste

situazioni si parla di cyberbullismo che si manifesta attraverso:

· invio di sms, mms, e-mail offensivi/e o di minaccia;

· dif fusione di messaggi offensivi ai danni della vittima, attraverso la divulgazione di sms o e-mail nelle mailing-list o nelle chat-line;

· pubbl icazione nel cyberspazio di foto o filmati che ritraggono prepotenze o in cui la vittima viene denigrate.

La rilevazione diretta degli indicatori da parte degli insegnanti o indiretta, sulla base di quanto riferito dagli alunni o dai genitori, deve affinarsi con l'osservazione delle relazioni interpersonali e delle possibili dinamiche conflittuali sottostanti presenti nel contesto classe, al fine di verificare l'entità e la natura del fenomeno e dare avvio al programma di intervento.

A chi segnalare:

L'attuazione del programma di intervento si basa prevalentemente sull'impiego delle risorse umane già presenti e disponibili: insegnanti e altro personale scolastico, alunni e genitori. Non serve, se non in casi particolarmente gravi, l'opera di psicologi, assistenti sociali, o altri specialisti a cui orientare la famiglia. L'elemento fondamentale per una buona riuscita del programma è infatti la corretta ristrutturazione del contesto relazionale degli alunni.

ABUSI SESSUALI

In particolare nel caso in cui ci si dovesse imbattere in materiale pedopornografico (cioè contenuti foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali), è necessario, innanzitutto, evitare di eseguire download, produrne copie, condividerne link o postarne il contenuto. Ciò è reato per chiunque. Nel venire a conoscenza di materiali di questo tipo è importante contribuire alla loro eliminazione: basta inserire le informazioni richieste sugli appositi modu l i onl i n e , disponib i li a i si t i www.sto p - i t .it e http://www.azzurro.it/it/clicca-e-segnala" ovvero collegandosi al sito della polizia postale https://www.commissariatodips.it, ove è possibile sia segnalare che denunciare. In alternativa è possibile recarsi nella sede più vicina della polizia giudiziaria. Ciò consente di operare con la massima tempestività. Non operare in modo isolato, ma confrontarsi con i colleghi di classe e il Dirigente Scolastico.

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.

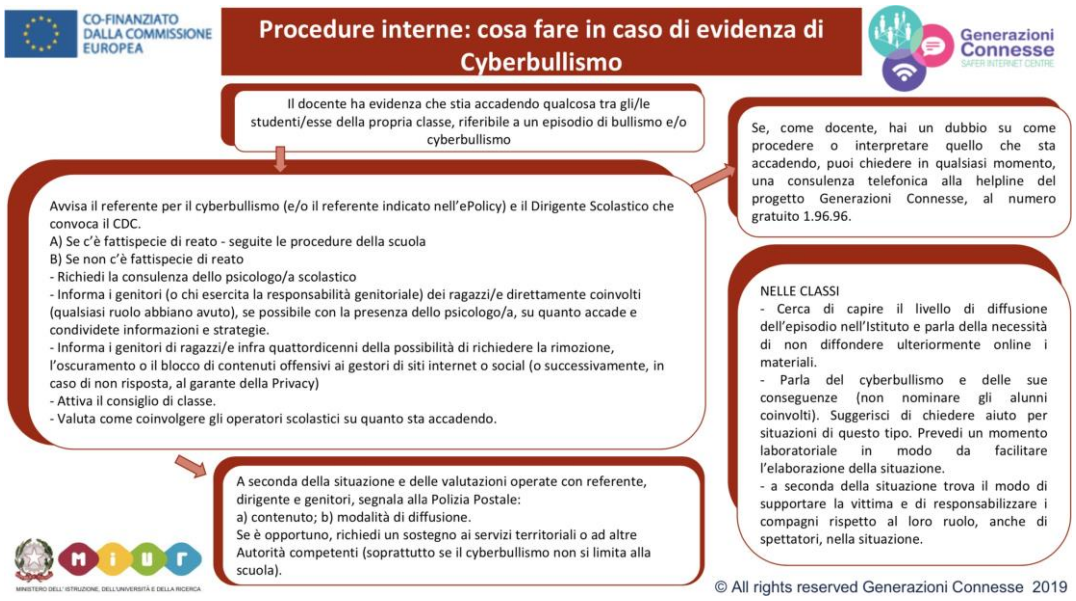
Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.

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

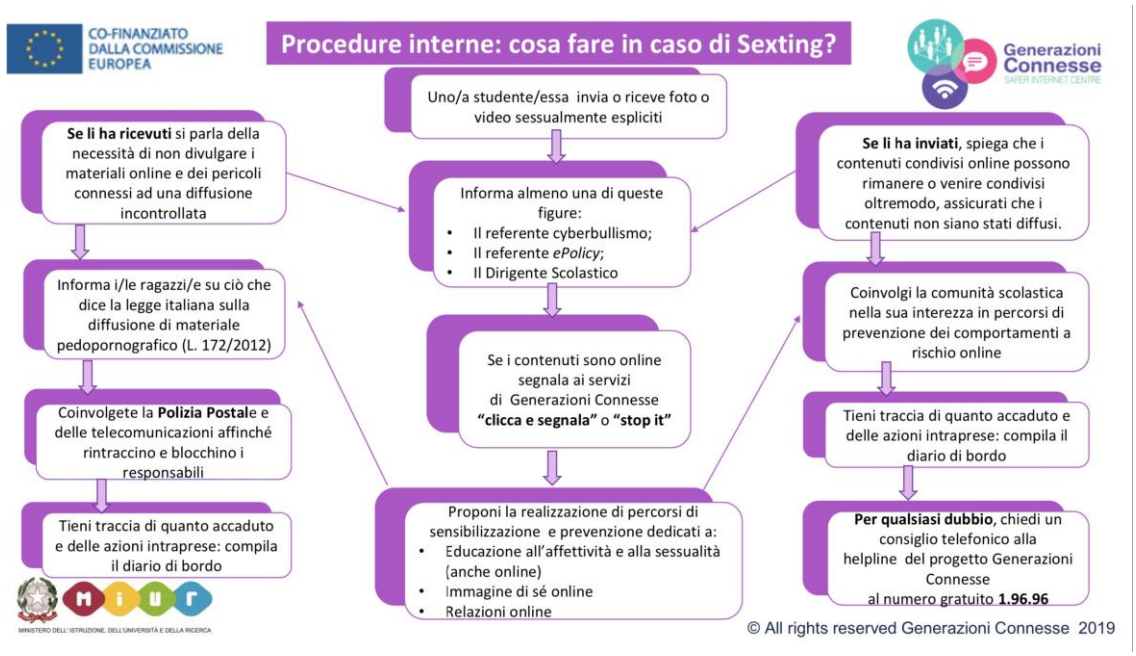
Il nostro Istituto 41 Console, ha attivato incontri con esperti esterni per sensibilizzare le famiglie dei nostri alunni alle numerose problematiche che nascono da una semplice navigazione sui social network.

5.4. *Allegati con le procedure*

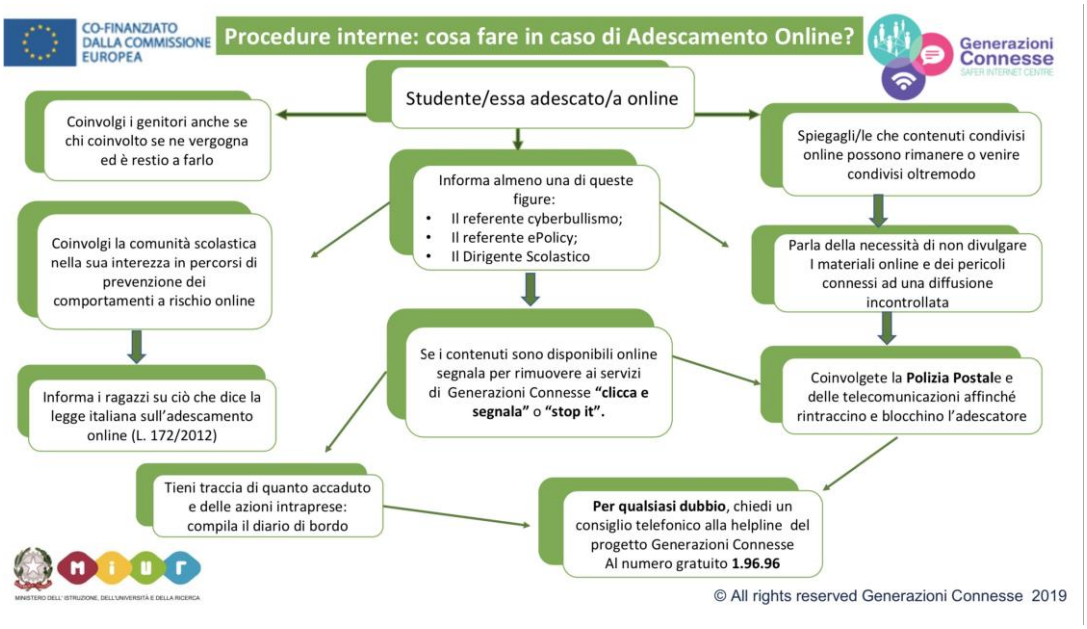
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



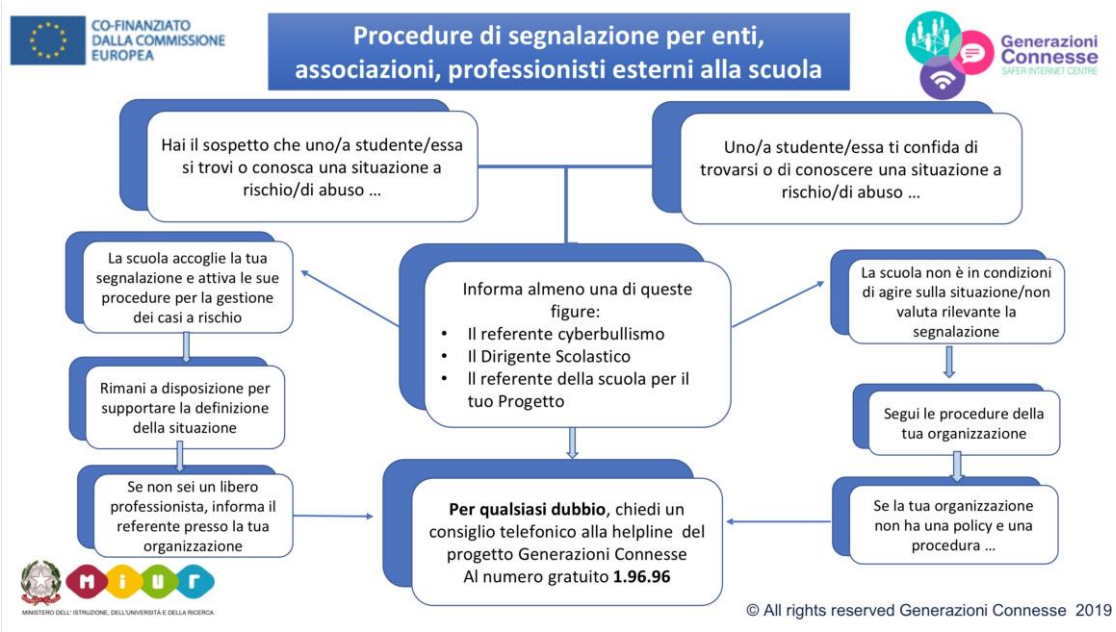
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

- Scheda di segnalazione

M.I.U.R.

NA I.C. 41 CONSOLE – NAPOLI -
Scuola dell'infanzia - Scuola primaria – Scuola Secondaria 1° Grado
Via Diomede Carafa, 28 – 80124 Napoli -
Uff. di segreteria 081 5702531
P.E. NAIC8CY00B@istruzione.it
P.E.C.: NAIC8CY00B@pec.istruzione.it
Cod. Mecc. NAIC8CY00B
C.F. 95170270631
www.41console.edu.it

UNIONE EUROPEA

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

Modello segnalazione/reclamo

cyberbullismo:https://www.41console.edu.it/c ategoria/modulistica-famiglie/1105/segnalazione-reclamo- cyberbullismo/

Guida sulle problematiche affrontate nel suddetto documento .

https://www.41console.edu.it/public/file/Opuscolo_Consigli_per_et%C3%A0_per_la Policy_di_E_Safe ty.pdf

Il nostro Istituto per aiutare gli alunni, i docenti, e le famiglie è stata creata una breve guida sulle problematiche affrontate nel suddetto documento .

Tale guida è presente sulla nostra pagina Webhttps://www.41console.edu.it/public/file/Opuscolo_Consigli_per_et%C3%A0_per_la Policy_di_E_Safety.pdf

Il Dirigente Scolastico
Prof.ssa Maria Patrizia Di Marco
Firma omessa ai sensi dell'Art. 3 comma 2 del D.L.G.V. 39/93

D.S