

I.T.T. "A. Pacinotti" - Taranto
Prot. 0017260 del 13/10/2025
I-1 (Entrata)



I.T.T. A.PACINOTTI

una scuola per il futuro



Via Lago Trasimeno, s.n.c. - Taranto - tel.0997369731 - C.F.90274490730
www.pacinottitaranto.edu.it - tatf09000g@istruzione.it - tatf09000g@pec.istruzione.it

Documento di ePolicy
I.T.T. A. PACINOTTI
Dirigente Scolastico
Dott.ssa Giovanna Santoro

Cap. 1 - Lo scopo della ePolicy

Capitolo 1 - Presentazione dell'ePolicy

1. Scopo dell'ePolicy
2. Ruoli e responsabilità nell'implementazione dell'ePolicy
3. Integrazione dell'ePolicy con regolamenti e normativa generale esistenti
4. Condivisione e comunicazione dell'ePolicy all'intera comunità educante
5. Gestione delle infrazioni all'ePolicy
6. I piani di Azione dell'ePolicy
7. Le risorse di Generazioni Connesse

Capitolo 2 - Sensibilizzazione e prevenzione

1. Sensibilizzazione e prevenzione
2. Il Curricolo Digitale
3. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (tecnologie dell'informazione e della comunicazione) nella didattica
4. Sensibilizzazione delle famiglie ed integrazioni al Patto di corresponsabilità
5. IL KIT DIDATTICO

Capitolo 3 - Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola

1. Protezione dei dati personali e GDPR
2. Accesso ad Internet
3. Strumenti di comunicazione online (PUA)
4. Strumentazione personale (BYOD)

Capitolo 4 - Segnalazione e gestione dei casi

1. Cosa segnalare
2. Come segnalare: quali strumenti e a chi
3. Gli attori sul territorio
4. Allegati con le procedure da seguire

Cap 1 - Scopo della ePolicy

1.1 Scopo dell'ePolicy

L' E-Policy ha come obiettivo principale quello di promuovere le competenze digitali per un uso delle tecnologie digitali positivo, critico e consapevole, da parte degli studenti e delle studentesse guidati dagli adulti coinvolti nel processo didattico-educativo. La competenza digitale è una competenza chiave del cittadino europeo come indicato dal Consiglio Europeo (Raccomandazione del 2018) che permette ad ogni cittadino di esercitare i propri diritti all'interno degli ambienti digitali (ONU - Commento Generale 25: I diritti dei minori negli ambienti digitali).

L'ePolicy è un documento programmatico che permette di lavorare su quattro obiettivi:

1. Il piano di azioni triennale per promuovere nell'intera comunità scolastica l'uso sicuro responsabile e positivo della rete;
2. le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
3. le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
4. le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

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 visione educativa e la proposta formativa dell'Istituto, 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 formativo ed 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 a rischio legate ad un uso non corretto delle tecnologie digitali.

1.2 ePolicy: ruoli e responsabilità dell'implementazione dell'ePolicy

Affinché l'ePolicy 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.

È opportuno che nel documento vengano definiti con chiarezza ruoli, compiti e responsabilità di ciascuna delle figure all'interno dell'Istituto.

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.

L'ITT PACINOTTI al fine di rispondere efficacemente a tale esigenza, individua le seguenti figure, declinando per ciascuna gli specifici ambiti di intervento:

IL DIRIGENTE SCOLASTICO

Il Dirigente Scolastico garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica. Segue corsi di formazione e di aggiornamento sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del Ministero dell'istruzione; promuove la cultura della sicurezza online e fornisce il proprio contributo all'organizzazione, insieme ai docenti referenti per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC. Presiede il Team per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo. Interviene nei casi bullismo, cyberbullismo ed uso improprio delle tecnologie digitali. Gestisce in prima persona, in collaborazione con i referenti e i docenti dei Consigli di classe, i casi gravi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

In merito alle attività di formazione sull'uso corretto delle nuove tecnologie e di prevenzione e contrasto dei fenomeni di bullismo e cyberbullismo, il Dirigente scolastico:

- definisce le linee di indirizzo del Piano Triennale dell'Offerta Formativa (PTOF) e del Patto

di Corresponsabilità (D.P.R. 235/07) affinché contemplino misure specificatamente dedicate alla prevenzione del bullismo e del cyberbullismo; favorisce l'adozione e l'aggiornamento di regole condivise inserite nel Regolamento di Istituto e di disciplina per il contrasto e la prevenzione dei fenomeni di bullismo e cyberbullismo;

- previene e contrasta fenomeni di bullismo e cyberbullismo nel rispetto della normativa vigente;
- assicura la massima informazione alle famiglie di tutte le attività e iniziative intraprese, anche attraverso una sezione dedicata sul sito web della scuola, che potrà rimandare al sito www.generazioniconnesse.it per tutte le altre informazioni di carattere generale;
- promuove, diffonde e coordina azioni educative e corsi di aggiornamento finalizzati a sensibilizzare l'intera comunità scolastica (studenti, genitori, personale non docente e docente) in materia di bullismo e cyberbullismo, a livello territoriale, anche in rete con enti, associazioni, istituzioni locali e altre scuole, coinvolgendo esperti;
- garantisce l'utilizzo sicuro di Internet a scuola, promuovendo la conoscenza sia dei contenuti tecnologici, sia delle implicazioni psicopedagogiche correlate;
- attiva specifiche intese con i servizi territoriali (servizi della salute, servizi sociali, forze dell'ordine, servizi minorili dell'amministrazione della Giustizia) in grado di fornire supporto specializzato e continuativo agli studenti coinvolti;
- nomina uno o più referenti per la prevenzione e il contrasto del bullismo e cyberbullismo, individuati dal Collegio dei Docenti.

L'ANIMATORE DIGITALE

L'Animatore digitale supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online e alla protezione e gestione dei dati personali, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale"; monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola, e ha il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password.

Secondo quanto disposto dall'art. 4 della Legge n. 71/2017, "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo", all'interno del personale docente dell'ITT Pacinotti sono stati individuati sei referenti: tre con il compito di coordinare le iniziative di prevenzione e di contrasto del bullismo e del cyberbullismo, tre come Team contro bullismo e cyberbullismo e dell'Emergenza.

In merito alle attività di formazione sull'uso corretto delle nuove tecnologie e di prevenzione e contrasto dei fenomeni di bullismo e cyberbullismo, il Team Referente bullismo e cyberbullismo:

- costituisce l'interfaccia con le forze di Polizia, con i servizi minorili dell'amministrazione della Giustizia, le associazioni e i centri di aggregazione giovanile sul territorio, per il coordinamento delle iniziative di prevenzione e contrasto del cyberbullismo;
- promuove azioni educative, iniziative e corsi di aggiornamento in materia di bullismo e del

cyberbullismo attraverso progetti d'Istituto che coinvolgano genitori, studenti e tutto il personale;

- coordina le attività di formazione sull'utilizzo corretto delle nuove tecnologie e, in particolare, sulle responsabilità di natura civile e penale, anche avvalendosi della collaborazione delle Forze di polizia, nonché delle associazioni e dei centri di aggregazione giovanile presenti sul territorio;
- si coordina con esperti esterni alla scuola (associazioni, servizi sociali e sanitari, aziende, forze dell'ordine, ecc.) per realizzare progetti di prevenzione;
- cura rapporti di rete fra scuole per eventuali convegni/seminari/corsi e per la giornata mondiale sulla Sicurezza in Internet ("Safer Internet Day");
- svolge un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'Istituto), atti e documenti (PTOF, PdM, Rav);
- raccoglie e diffonde le buone pratiche educative, organizzative e azioni di monitoraggio, favorendo l'elaborazione di un modello di ePolicy d'Istituto;
- partecipa a corsi di formazione, anche e tramite specifiche piattaforme sviluppate dal Ministero dell'Istruzione per i docenti referenti.

L'animatore digitale e il Team per l'Innovazione digitale sono co-responsabili, con il referente ePolicy, dell'attuazione dei piani di azione in particolare in riferimento alla formazione dei docenti. Sono inoltre responsabili del controllo all'accesso da parte degli studenti alle Tic.

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

E' una figura istituita dalla L. 71/2017, ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo, coinvolgendo, con progetti e percorsi formativi dedicati, studenti, colleghi e genitori. A tal fine, può avvalersi della collaborazione di partners esterni alla Scuola, quali Forze di Polizia, associazioni e centri di aggregazione giovanile presenti sul territorio.

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

In coerenza con le Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo del Ministero dell'Istruzione (D.M. n. 18 del 13/1/2021, agg. 2021 - nota prot. 482 del 18-02-2021), il Team ha le funzioni di coadiuvare il Dirigente Scolastico, coordinatore del Team nella scuola, nella definizione degli interventi di prevenzione e nella gestione dei casi di bullismo e cyberbullismo che si possono presentare. Promuove inoltre la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale e comunica ad alunni, famiglie e tutto il personale scolastico l'esistenza del team, a cui poter fare riferimento per segnalazioni o

richieste di informazioni sul tema.

Il Team ha il compito di:

- coadiuvare il Dirigente scolastico, coordinatore del Team, nella definizione degli interventi di prevenzione del bullismo (per questa funzione partecipano anche il presidente del Consiglio d'Istituto e i Rappresentanti degli studenti).
- Intervenire (come gruppo ristretto, composto da Dirigente e referente o referenti per il bullismo e il cyberbullismo, psicologo o pedagogo, se presente) nelle situazioni acute di bullismo.
- Promuovere la redazione e l'applicazione della ePolicy e monitorare le segnalazioni.

I/LE DOCENTI

Hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Adeguatamente informati e periodicamente aggiornati sulle problematiche attinenti alla sicurezza online e sulla politica adottata al riguardo dall'Istituto, devono integrare il curriculum della propria disciplina con approfondimenti inerenti tali buone pratiche, prevedere periodiche occasioni di confronto in aula con gli studenti guidandoli verso la maturazione di una coscienza digitale, e promuovere, laddove possibile, l'uso delle tecnologie digitali nella didattica. I docenti, inoltre, hanno il dovere morale e professionale di captare, monitorare e segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che veda coinvolti studenti e studentesse. Essi stessi devono gestire le comunicazioni digitali a carattere ufficiale nel rispetto del codice di comportamento professionale. I/le docenti osservano altresì regolarmente i comportamenti a rischio (sia dei potenziali bulli, sia delle potenziali vittime) e hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che veda coinvolti studenti e studentesse dandone tempestiva comunicazione al Dirigente Scolastico, al Referente per il Cyberbullismo e Bullismo e al Consiglio di Classe per definire strategie di intervento condivise, secondo il disposto normativo degli artt. 331 c.p.p. e 328 e 361 c.p.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Responsabile della protezione dei dati (RPD o DPO) conosce l'ePolicy di Istituto, fornisce la propria consulenza in merito agli obblighi derivanti dal GDPR e sorveglia sull'esatta osservanza della normativa in materia di tutela dei dati personali ed è co-responsabile delle azioni di informazione e formazione nell'Istituto sulla protezione dei dati personali

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

Svolge, in collaborazione con il DS e con il personale docente, funzioni di tipo amministrativo, contabile, gestionale e di sorveglianza connesse alla vita dell'Istituto e legate, direttamente o indirettamente, allo sviluppo di una cultura digitale. Adeguatamente formato in tema di bullismo e cyberbullismo, il personale ATA deve, come da specifici regolamenti d'Istituto, essere coinvolto nella segnalazione di comportamenti non adeguati e/o episodi conclamati, e fornire il proprio apporto nella raccolta, verifica e valutazione delle informazioni in merito.

GLI STUDENTI E LE STUDENTESSE

Gli studenti e le studentesse devono, in relazione al grado di maturità e consapevolezza raggiunta, impegnarsi ad utilizzare efficacemente e responsabilmente le tecnologie digitali, in coerenza con quanto richiesto dai docenti. Supportati dalla Scuola, devono comprendere l'importanza di adottare buone pratiche per tutelare la propria e l'altrui sicurezza online, partecipare attivamente a progetti ed attività che riguardino l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso, esternando liberamente difficoltà o richieste di aiuto dinanzi ad eventuali disagi emersi. I rappresentanti degli/delle studenti/studentesse sono informati del documento di ePolicy e invitati a costruire i piani di azione, a partire dal primo anno della secondaria di II grado.

I GENITORI/ADULTI DI RIFERIMENTO

I **Genitori**, in coerenza e continuità con la linea educativa adottata dall'Istituto in materia di TIC e Rete ed esplicitata in questo documento, devono promuovere in ambito domestico un uso consapevole, responsabile e rispettoso dei devices personali da parte dei propri figli, concordando con i docenti linee di intervento di carattere educativo in relazione ad eventuali problemi connessi ad un approccio inadeguato o pericoloso alle tecnologie digitali o a Internet. È estremamente importante che accettino e condividano quanto scritto nell'ePolicy d'Istituto e nel patto di corresponsabilità educativa in un'ottica di collaborazione reciproca. Si promuove il coinvolgimento dei rappresentanti di genitori/adulti di riferimento all'interno del percorso di definizione e implementazione dell'ePolicy.

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

Il mondo dell'associazionismo dovrà conformarsi alla politica della scuola riguardo all'uso consapevole delle TIC e della rete per la realizzazione di iniziative nelle scuole, finalizzate a promuovere un uso positivo e consapevole delle Tecnologie Digitali da parte dei più giovani,

e/o finalizzate a prevenire e contrastare situazioni di rischio online e valutare la rispondenza delle proposte di attività di sensibilizzazione/formazione alle esigenze di qualità contenute nel documento di ePolicy. Si dovrà inoltre promuovere comportamenti sicuri durante le attività che si svolgono con gli/le studenti/studentesse e verificare di aver implementato una serie di misure volte a garantire la tutela dei minori nel caso di insorgenza di problematiche e ad assicurarne la tempestiva individuazione e presa in carico.

1.3 Integrazione ePolicy nei documenti scolastici con la redazione di un'informativa per i soggetti esterni che erogano attività educative nell'Istituto

La trasversalità dell'ePolicy rende necessaria una sua integrazione nell'ambito dei documenti che disciplinano il funzionamento dell'Istituto Scolastico.

Il **Regolamento dell'Istituto scolastico**, che rappresenta il principale punto di riferimento normativo, dovrà essere aggiornato in modo tale da dare contezza dell'adozione dell'ePolicy, e richiamare le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione in ambiente scolastico. Il Regolamento d'Istituto viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

Il Dirigente scolastico, in collaborazione con i Referenti bullismo e cyberbullismo, valuterà la necessità di aggiornare periodicamente il Regolamento d'Istituto con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida del Ministero dell'Istruzione e le indicazioni normative generali.

Il Regolamento d'Istituto disciplina in modo dettagliato le tematiche in oggetto, e in particolare:

1. la Sezione che si occupa di regolare l'uso dei dispositivi elettronici e dei telefoni cellulari;
2. la Sezione che contiene un Regolamento specifico sul bullismo e il cyberbullismo.

Il personale scolastico si impegna a conoscere e ad applicare il Regolamento d'Istituto e gli eventuali aggiornamenti. A tale scopo partecipa periodicamente ad attività formative in materia di privacy e di utilizzo corretto dei dispositivi digitali.

Anche il **Patto di Corresponsabilità educativa** tra scuola e famiglia dovrà essere integrato con gli opportuni riferimenti all'ePolicy, puntualizzando, da un lato l'impegno dell'Istituto ad organizzare eventi formativi/informativi a beneficio dei genitori, e dall'altro l'impegno di questi ultimi a partecipare in maniera proattiva a tali eventi.

Il **Piano Triennale dell'Offerta Formativa**, per la sua funzione di carta d'identità culturale e

progettuale delle istituzioni scolastiche, nel quale si esplicita la progettazione curricolare, extracurricolare, educativa e organizzativa che le singole scuole adottano nell'ambito della loro autonomia, deve contenere anche le progettualità relative ad azioni media educative legate al percorso di ePolicy. Così come il PTOF è il risultato di una consapevole concertazione fra le componenti delle istituzioni scolastiche (Dirigente Scolastico, docenti, alunni, genitori) e fra queste e il territorio, il patto di corresponsabilità rappresenta l'assunzione di responsabilità da parte di tutti coloro che svolgono un ruolo attivo nella Comunità educante.

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 dello studente, ascoltare e prendere in seria considerazione le opinioni ed i desideri degli alunni, 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 a partecipare a comportamenti di minori che siano illegali, 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 dispositivi personali (smartphone, tablet, pc, ecc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto nel corso delle attività organizzate con gli studenti. 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). Al fine di rendere l'ePolicy uno strumento efficace per la tutela degli studenti e delle studentesse, si individua un insieme di regole o norme di comportamento da condividere con le organizzazioni/associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve e/o lungo periodo.

Le organizzazioni/associazioni extrascolastiche e gli esperti esterni sono tenuti a rilevare e a segnalare al Dirigente scolastico e ai Referenti bullismo e cyberbullismo le problematiche connesse ad un uso non corretto delle tecnologie digitali. In questo modo, si facilita l'intervento della scuola in chiave di prevenzione e di contrasto dei comportamenti scorretti e illeciti connessi all'utilizzo delle nuove tecnologie.

In coerenza con il percorso intrapreso e con le azioni che l'Istituto già pone in essere, la predisposizione di un'informativa sintetica sull'ePolicy comprensiva delle procedure di segnalazione garantisce un migliore rapporto fiduciario fra scuola e famiglia, consente di distinguere i ruoli e le azioni da compiere e di attivare direttamente, a seconda della tipologia dei casi da segnalare, le autorità competenti, collaborando con i servizi del territorio per la prevenzione e la gestione di quanto rilevato, in un'ottica di gestione condivisa degli interventi.

Tutti i soggetti esterni che erogano attività in ambito scolastico sono informati sui rischi online che possono correre gli studenti e le studentesse e sui comportamenti corretti che devono adottare a scuola.

I soggetti esterni sono tenuti a segnalare qualsiasi comportamento scorretto ai docenti responsabili del progetto, al Dirigente scolastico e ai Referenti bullismo e cyberbullismo, in qualsiasi forma, comunicando, per quanto possibile, i soggetti responsabili, le eventuali vittime, una descrizione il più possibile circostanziata dell'episodio. Per questo, i soggetti esterni possono compilare la scheda di segnalazione allegato alla fine del documento di ePolicy.

La presente informativa è condivisa con il personale e le associazioni esterne: le figure professionali e le organizzazioni coinvolte in progetti, laboratori e attività ne prendono visione e si impegnano a rispettarla preliminarmente all'avvio dei programmi con gli studenti, in classe o fuori.

1.4 Condivisione e comunicazione dell'ePolicy all'intera comunità educante

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

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

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

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene pubblicato sul sito istituzionale 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. Il documento di ePolicy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. Nello specifico è importante tener presente che:

- condividere e comunicare il documento agli studenti e alle studentesse significa dare loro una base di partenza per un uso consapevole e corretto dei dispositivi e della tecnologia

informatica;

- dare loro regole condivise di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici;
- dare loro elementi per poter riconoscere e quindi prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e.
- è importante condividere e comunicare il documento al personale scolastico in modo da poter orientare tutte le figure sui temi in oggetto, a partire da un uso corretto dei dispositivi e della Rete, in linea anche con il Codice di comportamento dei pubblici dipendenti;
- è fondamentale condividere con i genitori il documento e pubblicarlo sul sito istituzionale della scuola. La condivisione può avvenire anche tramite momenti di formazione specifici e durante gli incontri scuola-famiglia.

E' necessario, inoltre, che ciascun attore scolastico (dai docenti agli studenti) si faccia a sua volta promotore del documento.

Ogni Consiglio di classe si occupa di informare gli studenti della classe e di verificare che si adottino comportamenti corretti nell'utilizzo delle nuove tecnologie.

Tutti gli atti fondamentali dell'Istituto (Carta dei servizi, Regolamento d'Istituto, con particolare attenzione alla sezione bullismo e cyber bullismo, Regolamento di disciplina, Piano dell'offerta formativa triennale, ecc.) contengono una o più sezioni nelle quali sono esplicitati diritti e doveri degli operatori scolastici, degli alunni e dei genitori o di coloro che esercitano la responsabilità genitoriale. Tali documenti sono pubblicati sul sito dell'Istituto.

Il genitore, sottoscrivendo l'istanza d'iscrizione, assume l'impegno di:

- a) osservare le disposizioni contenute nel Patto di corresponsabilità e nel Regolamento d'Istituto;
- b) sollecitarne l'osservanza da parte dello studente.

Il genitore è consapevole che:

- a) le infrazioni disciplinari da parte dell'alunno possono dar luogo a sanzioni disciplinari;
- b) in caso di danneggiamenti o lesioni a persone, la sanzione è ispirata al principio della riparazione del danno (art. 4, comma 5 del DPR 249/1998, come modificato dal DPR 235/2007);
- c) il Regolamento d'Istituto disciplina le modalità d'irrogazione delle sanzioni disciplinari e i mezzi d'impugnazione verso i provvedimenti disciplinari.

All'inizio dell'anno scolastico, in occasione della presentazione del Regolamento d'istituto agli alunni da parte dei docenti, verrà analizzata la ePolicy d'Istituto. Nel corso dell'anno ogni docente dedicherà alcune lezioni alle buone pratiche per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta al cyber bullismo (anche nell'ambito delle attività di Educazione civica).

1.5 Gestione delle infrazioni alla ePolicy

La scuola gestisce le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora

fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

Nelle attività scolastiche ed extra-scolastiche gli studenti assumono i comportamenti richiesti dalle norme giuridiche, dallo Statuto delle studentesse e degli studenti e dal Regolamento di Istituto.

Il Regolamento d'Istituto, nel rispetto della normativa vigente, individua i comportamenti che configurano mancanze disciplinari, le relative sanzioni, gli organi competenti a irrogarle e il relativo procedimento.

I provvedimenti disciplinari hanno finalità educativa, tendono al rafforzamento del senso di responsabilità e al ripristino di rapporti corretti all'interno della scuola e sono ispirati, per quanto possibile, al principio della riparazione del danno.

In nessun caso può essere sanzionata, né direttamente né indirettamente, la libertà di espressione, qualora sia correttamente manifestata e non lesiva dell'altrui dignità e personalità. La responsabilità disciplinare è personale.

Nessuno può essere sottoposto a sanzioni disciplinari senza essere stato prima invitato a esporre le proprie ragioni. Lo studente ha facoltà di produrre testimonianze o elementi di prova a sé favorevoli.

Le sanzioni disciplinari sono sempre temporanee, proporzionate all'infrazione disciplinare, graduale e devono tenere conto della situazione personale dello studente. Le stesse dovranno avere finalità educative, puntando al rafforzamento del senso di responsabilità, al ripristino della corretta convivenza nella comunità scolastica e al recupero delle persone coinvolte. Tutti i provvedimenti che infliggono sanzioni disciplinari devono essere motivati oralmente e/o per iscritto.

Per quanto possibile, allo studente sarà offerta da parte dell'organo competente all'irrogazione, la possibilità di convertire la sanzione disciplinare in attività a favore della collettività, ossia socialmente utili. In caso di danni materiali, il responsabile o i genitori sono tenuti al risarcimento. In merito ai provvedimenti disciplinari, il Regolamento d'Istituto indica i mezzi di impugnazione (come il ricorso all'organo di Garanzia interno alla scuola) e i termini da rispettare.

A seconda dell'età degli studenti e in base alla gravità e alla diffusione di comportamenti devianti, si valuterà un intervento su tutto il contesto classe, con attività educative e di sensibilizzazione, anche per promuovere una maggior consapevolezza circa l'utilizzo delle TIC e di Internet. Si valuterà altresì l'opportunità di coinvolgere nell'azione educativa e formativa anche altri soggetti (psicologo scolastico, Rete di scuole, Polizia postale ecc.). Anche nei confronti del personale scolastico possono essere adottati provvedimenti disciplinari, in caso di uso improprio di dispositivi digitali e della Rete o in caso non intervenga o non segnali gravi comportamenti scorretti tenuti dagli studenti (cfr. artt 331 c.p.p., 328 c.p. e 361 c.p.)

1.6 I Piani di Azione dell'ePolicy

I piani di azione rappresentano il **programma triennale** di obiettivi che la scuola intende realizzare per promuovere la conoscenza delle regole e dei protocolli di intervento che sono stati adottati con il documento di ePolicy nella comunità scolastica. Nei Piani di Azione sono riportati **gli impegni e le responsabilità** che la scuola si assume per promuovere sui temi dell'educazione civica digitale e dell'utilizzo sicuro e consapevole delle tecnologie e della rete:

- la rilevazione dei bisogni
- le iniziative informative e formative,
- la formazione di docenti, studenti e studentesse e famiglie,
- il monitoraggio e la valutazione delle azioni (laddove possibile, anche all'interno del RAV);

I Piani di Azione si distinguono tra standard, comuni ad ogni scuola che ha adottato l'ePolicy, e autoprodotti ovvero definiti dalla scuola sulla base del proprio contesto territoriale e delle collaborazioni in essere con Istituzioni, associazioni e aziende.

L'E-policy viene aggiornata periodicamente, soprattutto 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 gruppo di lavoro. 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 Dirigente scolastico, in collaborazione con i docenti referenti per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo, valuterà periodicamente la necessità di procedere alla revisione e all'aggiornamento dell'ePolicy.

Il nostro piano d'azioni:

Azioni da svolgere entro un'annualità scolastica:

Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti

Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti

Azioni da svolgere nei prossimi 3 anni:

Organizzare un evento di presentazione del Progetto Generazioni Connesse rivolto agli studenti

Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto ai docenti

Organizzare un evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti

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

Organizzare un evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

1.7 Le risorse di Generazioni Connesse

Le risorse di Generazioni Connesse da utilizzare sono:

- Kit Didattico
- Area formazione (per docenti, famiglie, studenti/sse con ePolicy)
- Canale Youtube (webinar, video-stimolo, serie per target differenti) • Canale TikTok
- Canale Instagram • Canale Facebook

Cap 2 - Sensibilizzazione e prevenzione

2.1 Sensibilizzazione e prevenzione

La quotidianità in rete di ciascuno dei componenti della comunità scolastica - docenti, studenti e famiglie - deve essere caratterizzata da una consapevolezza critica delle caratteristiche degli ambienti e dei servizi online affiancata alle competenze per vivere al meglio il mondo connesso. In questa direzione l'ePolicy è un documento che sviluppa azioni e interventi con l'obiettivo di raggiungere l'intera comunità scolastica e promuovere, ciascuno secondo il proprio ruolo, una cittadinanza digitale composta dalla conoscenza dei diritti in rete, dei rischi e delle opportunità per una partecipazione attiva e responsabile nella rete.

Nell'ITT PACINOTTI, preliminarmente, l'Animatore digitale e gli Assistenti Tecnici si occupano anche di Misure di prevenzione dei rischi on line che riguardano:

1. Prevenzione riguardo alle minacce agli strumenti ICT: tenere aggiornato il sistema operativo dei dispositivi fissi e mobili connessi in rete installare e tenere aggiornato frequentemente il programma antivirus e browser, attivare la funzione firewall del S.O. (da pannello di controllo) connesso al server di rete tenere il livello di sicurezza a media - alto nelle impostazioni del browser per la navigazione nella rete internet;
2. Prevenzione riguardo agli accessi ad Internet: tenere riservate le credenziali (LOGIN e PASSWORD) di accesso alla rete Internet, tenere riservate le credenziali di accesso a servizi Internet, scegliere una password di almeno otto caratteri alfanumerici, non accedere ai siti web non certificati e nascosti (DEEP WEB), non aprire email con mittente sconosciuto e non scaricare allegati, non fornire proprie credenziali richieste tramite email (PHISHING);
3. Prevenzione riguardo normative privacy e copyright: formazione educativa sul rispetto della privacy delle persone (legge 196/2003), non fare foto e video senza autorizzazione delle persone ritratte o riprese, e se minorenni senza autorizzazione di entrambi i genitori, non pubblicare dati personali completi (cognome, nome, data e luogo di nascita propri ed altrui su social media, forum e siti web non conosciuti), non utilizzare prodotti intellettuali digitali (foto, video, e-book, etc) senza rispettare il copyright o creative commons nel web che non concedono il loro uso, non utilizzare dispositivi e non fare foto o videoregistrazioni se non autorizzati ai fini didattici dal

docente durante l'attività didattica. 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.

Al fine di promuovere l'acquisizione delle Digital skills, l'ITT PACINOTTI è impegnato da tempo nella realizzazione di azioni coerenti con il PNSD prima ed il PNRR oggi (DM 65/2024, DM 170/2024 e DM 19/2024), ha ampliato e integrato la propria offerta formativa con specifici rimandi al tema, pianificando interventi che integrano la dimensione tecnologica, afferente l'acquisizione di saperi di base, con quella cognitiva, legata all'acquisizione e al trattamento dell'informazione, e quella etica, mirante a promuovere un'interazione sociale corretta e responsabile.

L'ITT PACINOTTI nel corso di questi anni, inoltre:

- ha aderito ogni anno al SID (Safer Internet Day);
- ha partecipato in presenza, durante la tappa di Taranto, a "Una vita da social", la campagna educativa itinerante della Polizia di Stato e del Ministero dell'Istruzione nell'ambito del progetto "Generazioni Connesse";
- ha consigliato costantemente l'App YouPol agli oltre 1000 alunni frequentanti il nostro Istituto;
- ha illustrato il protocollo "1000 occhi sulla città" promosso dal Ministero dell'Interno
- ha effettuato un'attività di sensibilizzazione prevalentemente nelle classi del primo biennio con alcuni interventi miranti alla sensibilizzazione della lotta ed il contrasto del bullismo e del cyberbullismo.

2.2 Il Curricolo Digitale

Per realizzare questo obiettivo l'istituto utilizza le risorse messe a disposizione a livello nazionale e internazionale.

Nello specifico il curriculum delle competenze digitali si è sviluppato secondo le 5 aree del quadro di riferimento DIGCOMP (Quadro comune di riferimento europeo per le competenze digitali):

1. **ALFABETIZZAZIONE SU INFORMAZIONI E DATI:** navigare e ricercare in rete, filtrare i contenuti e le informazioni, gestirne l'elaborazione.
2. **COMUNICAZIONE e COLLABORAZIONE:** utilizzare le tecnologie digitali per condividere i contenuti, per collaborare senza ledere l'identità digitale altrui.
3. **CREAZIONE DI CONTENUTI DIGITALI:** integrare, rielaborare e sviluppare contenuti digitali rispettando copyright e licenze.
4. **SICUREZZA:** creare un ambiente protetto utilizzando account personalizzati e blocchi, in modo da proteggere i dati e la privacy.
5. **RISOLVERE PROBLEMI:** monitorare i fabbisogni individuali, risolvere problemi tecnici; individuare fabbisogni e risposte tecnologiche; utilizzare in modo creativo le tecnologie digitali; individuare divari di competenze digitali.

Il DigComp 2.2, framework europeo sulle competenze digitali, permette di costruire una cornice precisa in cui inquadrare i temi e le corrispondenti competenze da proporre nell'Istituto non solo per gli studenti. Al suo interno vengono identificati alcuni temi sui quali è costruita una proposta specifica per le famiglie e gli studenti (formazione). Tale cornice trova poi sviluppo specifico, per gli studenti, nel curriculum di educazione alla Cittadinanza Digitale previsto dalla L. 92/2019. Il curriculum prende forma attorno all'ePolicy e le attività didattiche sono legate al documento ed alle scelte dell'Istituto al suo interno. Nel curriculum va previsto in ogni classe un appuntamento didattico specifico, calibrato sull'età degli alunni, e l'utilizzo dei kit didattici per favorire da parte degli studenti una maggiore conoscenza e consapevolezza delle finalità del presente documento. I regolamenti e le attività sviluppate sul tema della prevenzione presenti nell'ePolicy sono parte, costante ma non esclusiva, delle azioni di disseminazione e sensibilizzazione descritte ed attuate dall'Istituto.

2.3 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.

Il nostro Istituto è Polo di Formazione Ambito 21 nella città di Taranto e Provincia (per la formazione del personale neo immesso in ruolo), è uno dei Poli formativi nazionali del PNRR per quanto riguarda la transizione al Digitale (i corsi previsti nei DM 84750/23 e DM 66/2024 sono fruibili in presenza o in modalità blended o on line su Piattaforma Scuola Futura) e negli ultimi anni ha promosso e realizzato iniziative di formazione dei docenti sull'utilizzo ed integrazione delle TIC nella didattica e tenendo conto di quanto previsto dal programma del PNRR.

Nella prospettiva del miglioramento dell'offerta formativa il percorso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica deve diventare, dunque, un processo permanente, in modo che le conoscenze siano il più possibile diffuse e condivise tra i docenti, sia attraverso momenti di autoformazione, che di formazione collettiva. Questo può avvenire incentivando la partecipazione dei docenti a tutte quelle iniziative di formazione su questi temi, promosse sia a livello ministeriale, che dagli Ambiti Territoriali.

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.

Il percorso della formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet prevede momenti di formazione, personale o collettiva, che devono integrare e potenziare le competenze tecnologiche e che delle modalità di comunicazione.

Per realizzare tali interventi la scuola agirà su vari fronti:

1. organizzare corsi interni, sia predisposti dall'istituto che da scuole all'interno dell'Ambito Territoriale per l'acquisizione di conoscenze e di approcci responsabili di fronte alle nuove tecnologie digitali, in considerazione del ruolo fondamentale che il docente assume in questo processo;
2. favorire la partecipazione a corsi esterni inerenti all'uso consapevole della Rete e delle tecnologie digitali che rispondano ad esigenze formative della scuola nel suo complesso.
3. informare i docenti su iniziative di formazione a distanza;
4. organizzare incontri con esperti esterni, in forma di seminari o dibattiti, che coinvolgano tutto il corpo docente

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 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.

Per favorire la sinergia degli interventi educativi di scuola e famiglia e garantire il successo della prevenzione dei rischi connessi ad un uso non consapevole delle TIC è necessaria la collaborazione di tutti gli attori educandi, ognuno secondo i propri ruoli e le proprie responsabilità.

Altrettanto importante è la promozione di un uso consapevole delle TIC, capace di cogliere le opportunità offerte delle nuove Tecnologie. Per questa ragione il nostro Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sulle tematiche delle tecnologie digitali previste dall'ePolicy e dal suo piano di azioni. Pertanto il presente documento è messo a disposizione di tutta la comunità scolastica sul sito web d'Istituto assieme al Patto educativo di corresponsabilità stipulato con le famiglie. Tale documento costituisce l'impegno reciproco alla corresponsabilità formativa, nella quale rientrano pienamente i temi legati alla ePolicy.

La scuola intende valorizzare le opportunità di incontro e formazione per le famiglie sui temi oggetto della ePolicy, selezionando iniziative significative promosse da Enti e/o Associazioni presenti sul territorio.

Si promuoveranno momenti di confronto e discussione anche sulle dinamiche che potrebbero crearsi fra pari con l'uso di smartphone e social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo e dei risvolti correlati ad un'inappropriata navigazione in rete.

2.5 Il Kit Didattico

L'e-Policy prevede, a livello macro, un lavoro di lettura e d'intenti condivisi dall'intera comunità scolastica, a livello micro, invece, immagina che la singola classe lavori anche su tematiche direttamente collegate alla sicurezza in rete, ma complesse e di non immediata

ricaduta nelle programmazioni scolastiche (etica e digitale, algoritmi, datafication). A tal fine si è progettato e predisposto del materiale che possa funzionare sia da attivatore, sia d'accompagnamento ai docenti e agli studenti nella fase più delicata ed incisiva del processo di prevenzione: la lezione in classe. Pertanto, il progetto Generazioni Connesse, a supporto del lavoro dell'e-Policy ha previsto per i docenti e studenti di ogni segmento scolare un nuovo Kit Didattico che contiene materiali per le lezioni e per il proprio aggiornamento, a partire dalla scuola d'infanzia fino alla secondaria di secondo grado. Il Kit può essere usato nella sua interezza oppure può essere oggetto di selezione e scelta, sulla base di quanto fatto dal docente.

Cap 3 - Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola

3.1 Protezione dei dati personali e GDPR

“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 ed 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). 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. In particolare, la scuola non ha solo il compito di tutelare la privacy degli/le studenti/esse e delle loro famiglie, ma anche quello di informare e soprattutto rendere consapevoli gli studenti di quanto sia importante tutelare il diritto alla riservatezza di se stessi e degli altri. La diffusione sempre maggiore di smartphone tra i giovanissimi, l'uso di tablet a scopo didattico, la condivisione online di contenuti didattici, l'uso del registro elettronico, l'eventualità di gruppi Whatsapp tra studenti, genitori, docenti o

tra insegnanti e studenti, obbligano la scuola ad avere un'attenzione particolare non solo alla privacy in generale, ma anche alla gestione della privacy legata all'uso dei nuovi dispositivi. La velocità, l'immediatezza con cui si risponde ai messaggi o si condividono foto o video, può far perdere il controllo di dati personali e mettere a rischio la reputazione e la sicurezza dei soggetti coinvolti. I principali obblighi in materia di protezione dei dati personali consistono nella definizione di un "organigramma privacy", nel rilascio dell'informativa al momento della raccolta dei dati e nella tenuta di un registro dei trattamenti.

3.2 Accesso ad Internet

"L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.

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. Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.

L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite. 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 ed inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

Il regolamento, dunque, deve prevedere una parte dedicata all'uso di Internet in cui gli **studenti** si impegnano a:

- ✓ Utilizzare la rete nel modo corretto.
- ✓ Rispettare le consegne dei docenti.
- ✓ Non scaricare materiali e software senza autorizzazione.
- ✓ Non utilizzare unità removibili personali senza autorizzazione.
- ✓ Tenere spento lo smartphone al di fuori delle attività didattiche che ne prevedano l'utilizzo.
- ✓ Durante le attività che prevedono lo smartphone, utilizzarlo esclusivamente per svolgere le attività didattiche previste.
- ✓ Segnalare immediatamente materiali inadeguati ai propri insegnanti.

I **docenti** si impegnano a:

- ✓ Utilizzare la rete nel modo corretto.
- ✓ Non utilizzare device personali se non per uso didattico. Formare gli studenti all'uso della rete.
- ✓ Dare consegne chiare e definire gli obiettivi delle attività.
- ✓ Monitorare l'uso che gli studenti fanno delle tecnologie a scuola.

Checklist per:

- ✓ Mantenere separate le reti didattica e segreteria.
- ✓ Aggiornare periodicamente software e sistema operativo.
- ✓ Definire la programmazione di backup periodici.
- ✓ Garantire formazione adeguata allo staff, incluso il corpo docenti. Testare regolarmente le possibili vulnerabilità.
- ✓ Preparare piani di azione in risposta ai problemi più seri.
- ✓ Predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo.

3.3 Strumenti di comunicazione online (PUA)

La Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) è un documento che racchiude una serie di regole legate all'utilizzo della rete a scuola e a casa da parte di studenti e di tutto il personale (compresi i professionisti esterni che lavorano in contesto scolastico), integrante il DPS (Documento programmatico sulla Sicurezza). Il documento, che funge da raccordo, si compone di punti strategici riguardanti non solo i vantaggi di internet a scuola ma anche i rischi connessi all'online, nella valutazione di quei contenuti presenti in rete e di quelle azioni negative che possono comprometterne l'uso positivo. Fra queste attività: ricercare materiale non consono allo stile educativo della scuola; produrre vere e

proprie azioni illecite; giocare online con la rete scolastica; violare la privacy e i diritti d'autore, etc... Nella Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) vengono definite, dunque, le regole di utilizzo fra tutti gli attori in gioco, nel rispetto dei dati sensibili di ciascuno, in particolar modo degli alunni e delle alunne. Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

L'ITT Pacinotti adotta da tempo vari strumenti di comunicazione online, sia per raggiungere target esterni, al fine di valorizzare e promuovere le attività portate avanti dall'Istituto trasmettendo all'esterno l'identità, i valori, l'idea di educazione fatte proprie dalla Scuola, sia per far circolare al suo interno, fra i diversi attori scolastici, informazioni di servizio o contenuti importanti.

Per quanto riguarda, nello specifico, gli strumenti di comunicazione interna, l'Istituto adotta le seguenti modalità telematiche:

- nella gestione delle relazioni scuola/famiglia, si fa ricorso al Registro elettronico, strumento principe della comunicazione in contesto scolastico, accessibile da entrambi gli utenti tramite credenziali personali. È possibile la prenotazione informatizzata dei colloqui con i docenti da parte dei genitori, nonché l'inoltro e la ricezione di documentazione riguardante la vita della scuola. In relazione a quest'ultimo aspetto, è assicurata alle famiglie, nel rispetto delle norme di riservatezza, l'informazione trasparente e tempestiva sul processo di apprendimento e sulla valutazione degli alunni effettuata nei diversi momenti del percorso scolastico;
- nella gestione dei rapporti dirigenza/personale i canali comunicativi privilegiati sono la posta istituzionale e l'area riservata del Registro elettronico che i docenti si impegnano quotidianamente a controllare;
- la comunicazione docenti/alunni avviene attraverso aree dedicate del Registro elettronico, accessibili da entrambi tramite credenziali personali. È possibile condividere materiale didattico con i docenti e, anche in questo caso, avere accesso a informazioni in modo trasparente e tempestivo.

Ad integrazione dei predetti canali comunicativi, i docenti, gli studenti e le famiglie utilizzano anche le funzionalità della piattaforma Google Workspace che consente di svolgere a distanza riunioni di carattere didattico e organizzativo, all'uopo l'ITT Pacinotti, in data 26 ottobre 2023, ha deliberato un apposito Regolamento che disciplina proprio lo svolgimento delle dette riunioni.

La piattaforma individuata risponde ai necessari requisiti di sicurezza dei dati a garanzia della privacy, assicura un agevole svolgimento dell'attività sincrona e risulta fruibile da qualsiasi tipo di device. L'accesso al servizio avviene mediante credenziali personali (i genitori, in particolare, utilizzano l'account dei propri figli).

A seguito della determina n. 36 del 12 febbraio 2018 emanata dall'Agenzia per l'Italia Digitale e in coerenza con quanto stabilito dal Piano Triennale per l'informatica, l'istituto Pacinotti ha modificato la struttura e le funzionalità del proprio sito, oggi con estensione "edu.it", con l'obiettivo di:

- migliorare la visibilità, l'accesso alle informazioni e ai servizi online esistenti;
- introdurre nuove aree in modo da offrire all'utenza interna ed esterna tutti i servizi previsti dalla normativa vigente;
- accrescere la sicurezza dei dati trattati.

La nuova veste grafica, chiara e semplice, rispetta tutti gli obblighi di trasparenza per le Pubbliche Amministrazioni che hanno standardizzato la modalità di pubblicazione dei contenuti, indicando per ognuno di essi la posizione e la denominazione all'interno dei siti istituzionali delle medesime; i menu di navigazione sono pertanto suddivisi per categorie in cui reperire facilmente le informazioni sulla nostra Scuola, sulla sua organizzazione, sulle attività proposte, sui progetti, sulle attività PCTO ed altro ancora.

3.4 Strumentazione personale (BYOD)

La presente ePolicy conterrà 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 MIM per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device"). Risulta infatti 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.

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 PNRR.

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.

L'utilizzo di strumentazione personale in contesto scolastico si lega oggi strettamente al principio dell'autonomia scolastica e viene normato dai singoli regolamenti di Istituto.

In riferimento alla vexata quaestio connessa all'impiego dello smartphone da parte degli studenti durante lo svolgimento delle attività didattiche, il Regolamento di Istituto prevede che i dispositivi possono essere utilizzati solo durante lo svolgimento delle attività didattiche e previa espressa autorizzazione dei docenti, così come previsto dalla Disposizione Ministeriale prot. 3392 del 16.06.2025 (<https://www.mim.gov.it/-/circolare-n-3392-del-16-giugno-2025>) Quanto al personale docente, l'impiego di devices personali in classe è consentito unicamente per fini didattici e professionali. In tal caso la responsabilità in merito alla conservazione e corretta gestione degli stessi è affidata unicamente al proprietario. Analoghe riflessioni si applicano alle altre figure operanti a vario titolo nella Scuola: ne è autorizzato l'impiego a patto che non intralci o distraiga dal regolare svolgimento delle proprie mansioni.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2025/2026)

Sensibilizzare, mediante sessioni informative in orario curricolare, gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

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

Cap 4 - Segnalazione e gestione dei casi

4.1 Cosa Segnalare

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. Queste, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola. Nelle procedure sono indicate le figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso, nonché le modalità di coinvolgimento del Dirigente Scolastico e del Referente per il contrasto al bullismo e al cyberbullismo. 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.** 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.

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 diffusione delle tecnologie digitali e dell'accesso alla Rete fra i più giovani è all'origine di profondi cambiamenti nelle dinamiche relazionali e in quelle identitarie: mutano linguaggi, modalità di comunicazione, abitudini e stili di vita, si offrono inedite potenzialità di crescita. Al tempo stesso, tuttavia, come già ampiamente dibattuto, questi nuovi e privilegiati strumenti di partecipazione portano in primo piano il delicato tema della "sicurezza" e del comportamento sociale. Siamo, evidentemente, di fronte ad una realtà complessa, nella quale, accanto a nobili fini, trovano spazio contenuti e comportamenti potenzialmente dannosi, sfocianti talvolta in veri e propri reati, dal Cyberbullismo all'Hate speech, dalla Dipendenza da Internet ai Giochi online, dal Sexting al Grooming alla Pedopornografia online. Occorre, pertanto, demolire lo stereotipo dei giovani "competenti" a priori e, piuttosto, promuovere in loro l'acquisizione delle necessarie competenze e capacità affinché possano adeguatamente proteggersi, fruire dei nuovi media con consapevolezza, sfruttare le potenzialità delle tecnologie digitali e gestirne le implicazioni.

La responsabilità dell'azione preventiva ed educativa coinvolge diverse agenzie formative, in primis la famiglia e la scuola. La necessità di supportare un uso positivo e consapevole delle TIC da parte dei più giovani, sia in un'ottica di tutela dai rischi potenziali che nella valorizzazione delle opportunità esistenti, pone entrambe di fronte alla sfida di riconsiderare la propria identità, il proprio ruolo educativo e le proprie risorse, oltre allo stato dei rapporti reciproci per un patto educativo da rinnovare costantemente.

L'Istituto A. Pacinotti in particolare, intende rafforzare la sua capacità di rispondere a questi nuovi bisogni attraverso strumenti e misure specifiche, dando una risposta il più possibile integrata, che trovi la sua espressione di indirizzo in procedure chiare di cui la Scuola dovrà dotarsi e che includano la collaborazione con la rete dei servizi locali (in primis le ASL e la Polizia Postale).

È opportuno, inoltre, che i docenti, nell'espletamento delle proprie funzioni di formatori ed educatori sappiano cogliere ogni opportunità per riflettere insieme agli alunni su tali rischi. Fondamentale monitorare costantemente le relazioni interne alla classe, onde individuare possibili situazioni di disagio ed intervenire tempestivamente, anche mediante il ricorso alle figure di sistema specializzate, nonchè allo Sportello d'ascolto attivo da anni presso l'Istituto, al fine di venire incontro alle specifiche esigenze del singolo. Per questo motivo il nostro Collegio dei Docenti con la delibera n. 36 del 16 maggio 2025 ha approvato il modulo inerente le segnalazioni per combattere proprio il verificarsi di questi fenomeni. Alla stesura dello stesso il nostro Istituto ha partecipato con costanza e fattivamente formulando proposte nei

diversi incontri programmatici indetti dal Garante dei Diritti del Minore della Regione Puglia, dott. Ludovico Abbaticchio.

Tale percorso interno potrà essere ulteriormente rinforzato dalla partecipazione a progetti e/o iniziative esterne coerenti con i temi sopra menzionati, cui la Scuola porrà particolare attenzione, selezionando eventi significativi promossi da Enti e/o Associazioni di comprovata affidabilità.

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 da individuare all’interno dei rappresentanti di istituto o di ulteriori alunni particolarmente sensibili alla suddetta problematica; 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 contrapposizione al 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).

Spesso studenti/sse e genitori ritengono che tutto ciò che avviene online, proprio perché si colloca fuori dalle aule, non debba riguardare l'Istituzione scolastica. Tale pregiudizio coinvolge sia chi è vittima di cyberbullismo, che non ritiene di segnalare le offese ricevute nei social, magari perché effettuate da studenti di altri Istituti scolastici, sia chi pratica forme di cyberbullismo, che si considera al sicuro proprio perché opera da casa o comunque fuori dall'ambito scolastico. Al contrario bisogna diffondere la consapevolezza che la scuola rappresenta l'Istituzione più vicina ai giovani, il luogo dove quotidianamente essi vivono e si formano, e che, in virtù anche della legge 71/2017, essa è pronta ad accogliere qualsiasi tipo di segnalazione attraverso il personale preposto e attraverso strumenti e modi formalizzati nel presente documento.

“La scuola c'è” dovrebbe essere il messaggio interiorizzato da tutti per far fronte al disagio e alla sofferenza di chi è vittima di cyberbullismo, di adescamento online, di sexting o di qualsiasi forma di violenza, aggressione, pressione psicologica che avvenga a danno di uno/una studente/ssa attraverso l'uso di social media.

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 (prot. OSCAD)

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 coscienza consapevole e costruttiva da parte dei giovani.

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 e intende attuare un monitoraggio degli studenti e delle studentesse per effettuare, se necessario, degli interventi personalizzati di sostegno e di aiuto.

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 medialmente 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.

L'Istituto effettuerà degli incontri con la Polizia Postale e/o esperti al fine di informare e sensibilizzare gli studenti e le studentesse sulla problematica e attuerà un monitoraggio costante per effettuare, se necessario, degli interventi personalizzati di sostegno e di aiuto.

Adescamento online

Il grooming (dall'inglese “groom” - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenzialmente 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 ed 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.

L'Istituto prevede, all'interno della programmazione di Educazione Civica, la trattazione di questo argomento, inoltre effettuerà degli incontri con la Polizia Postale e con i Carabinieri al fine di informare e sensibilizzare gli studenti e le studentesse sulla problematica. Si effettueranno anche monitoraggi per rilevare eventuali casi critici e attivare interventi personalizzati di sostegno e di aiuto.

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, concreti

o simulati o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali, appunto. La legge n. 269 del 3 agosto 1998 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.

L’istituto prevede, all’interno della programmazione di Educazione Civica, la trattazione di questo argomento nell’ambito della tematica relativa alla Cittadinanza digitale. Si effettueranno anche monitoraggi per rilevare eventuali casi critici e attivare interventi personalizzati di sostegno e di aiuto

Il nostro piano d’azioni

AZIONI (da sviluppare nell’arco di un anno).

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all’utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il

coinvolgimento di esperti.

- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.
- Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

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

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.
- Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

4.2 Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale (ex art. 357 c.p.) 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. Il Codice Penale Italiano, all'art. 357, definisce il pubblico ufficiale come colui che esercita una "pubblica funzione legislativa, giudiziaria o amministrativa". Questa definizione si estende ai docenti nel momento in cui sono impegnati nell'esercizio delle loro funzioni all'interno degli istituti scolastici. La Corte di Cassazione, con la [sentenza n. 15367/2014](#), ha ribadito la qualifica di pubblico ufficiale per l'insegnante, estendendo tale riconoscimento non solo alla tenuta delle lezioni, ma anche a tutte le attività connesse. Questo include, ad esempio, gli

incontri con i genitori degli allievi. Le situazioni problematiche in relazione all'uso delle tecnologie digitali sono gestite da un team di docenti composto da:

1. Dirigente
2. L'animatore digitale (secondo il Piano Nazionale per la Scuola Digitale, abbreviato in PNSD, introdotto dalla Legge 107/2015)
3. Referente bullismo (ex. Legge Italiana Contro il Cyberbullismo, L. 71/2017)
4. Altri docenti già impegnati nelle attività di promozione dell'educazione civica.

Le situazioni di pregiudizio presunto o reale possono richiedere il supporto e l'intervento di esperti esterni alla scuola.

Esaminando la realtà, si potrebbero palesare due macro - 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.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l'obiettivo di allertare il Dirigente. La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, il Dirigente e i docenti coinvolti procedono alla valutazione del caso (valutare l'invio o meno della relazione agli organi giudiziari preposti) e agiscono tramite percorsi di sensibilizzazione.

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.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" al fine di allertare il Dirigente. La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, si procede alla valutazione approfondita e alla verifica di quanto segnalato, avviando (se appurato la rilevanza penale) la procedura giudiziaria con denuncia all'autorità giudiziaria per attivare un procedimento penale.

Qualora si rilevasse un fatto riconducibile alla fattispecie di reato, l'insegnante - nel ruolo di pubblico ufficiale - non deve procedere con indagini di accertamento ma ha sempre l'obbligo di segnalare l'evento all'autorità giudiziaria. (ex. l. 71/2017).

Con autorità competente si intendono:

Procure Ordinarie: nel caso in cui il minore/i sia la vittima/e ed il presunto autore del reato sia maggiorenne;

Procura Minorile: in caso il presunto autore del reato sia minorenne.

Vi è anche l'obbligatorietà della segnalazione delle situazioni di pregiudizio a carico dei minori: L. 216/1991: per le situazioni di grave rischio l'istituzione scolastica è tenuta alla segnalazione delle medesime. Per pregiudizio si intende una condizione di rischio o grave difficoltà che provocano un danno reale o potenziale alla salute, alla sopravvivenza, allo sviluppo o alla dignità del bambino, nell'ambito di una relazione di responsabilità, fiducia o potere. La segnalazione come da procedura interna è il primo passo per aiutare un minore che vive una situazione di rischio o di grave difficoltà e va intesa come un momento di condivisione e solidarietà nei confronti del minore. La mancata segnalazione costituisce, infatti, omissione di atti d'ufficio (art.328 C.P.) oltre l'omessa denuncia (artt. 361 c.p. e 331 c.p.p.). Può essere utile, valutando accuratamente ciascuna situazione, attivare colloqui individuali con tutti i minori coinvolti, siano essi vittime, testimoni e/o autori. È importante considerare il possibile coinvolgimento dei genitori e di coloro incaricati della tutela dei minori coinvolti. L'intervento va indirizzato valutando l'eventuale impatto educativo e/o il contesto emotivo senza discriminare tra vittime, testimoni e/o autori. Prevedere possibili incontri di mediazione tra i minori coinvolti vanno ponderati con la consapevolezza del loro stato emotivo, anche e in base agli elementi raccolti in merito del fatto/episodio avvenuto (elementi che si dovrebbero valutare di caso in caso). Importante è prevedere il coinvolgimento dei genitori sia della vittima che del bullo (ove possibile). Anche i genitori devono e possono segnalare casi di sospetto o evidenza dei fenomeni, segnalarlo al Dirigente o al docente coordinatore di classe o referente di istituto oppure direttamente al team antibullismo, attraverso apposita procedura che definisce l'istituto (mail ad hoc, tramite gli uffici e postazioni specifiche, etc...).

Gli insegnanti e i genitori, come studenti e studentesse, si possono rivolgere alla Helpline del progetto Generazioni Connesse, al numero gratuito 19696, attraverso la chat disponibile sul sito o tramite chat WhatsApp per ricevere supporto e consulenza.

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. Particolare attenzione deve essere data alle chat di classe che utilizzano cyberbullismo quali:

- L'esclusione (quando a uno/a studente/ssa della classe si impedisce di partecipare alla chat o lo si allontana);
- Le offese o le prese in giro reiterate;

- Le imposizioni quali l'intimazione a passare dei compiti o a farsi interrogare.

Per questo motivo è necessaria una vigilanza dei genitori che sono gli unici a poter accedere alle chat frequentate dai figli e che, attraverso un dialogo costante, dovrebbero monitorare se la chat di classe è usata correttamente o no. Si ricorda infatti che il ruolo dei cosiddetti “spettatori” (cioè di coloro che assistono o sono a conoscenza che all'interno della classe sono presenti atti di bullismo) è fondamentale.

Spesso la vittima, per vergogna o perché si trova in una situazione di fragilità, non trova il coraggio di denunciare i cyberbulli o di appellarsi agli insegnanti. E' dunque responsabilità di tutti gli studenti, con l'appoggio dei genitori che rappresentano la prima “agenzia educativa”, farsi carico delle segnalazioni.

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. In particolare, la scuola ha già attivato sistemi di segnalazione utili anche al monitoraggio dei fenomeni dal quale partire per integrare azioni didattiche preventive e giornate di sensibilizzazione, insieme agli Enti/Servizi presenti sul territorio di riferimento.

Da lungo tempo l'Istituto Pacinotti si è dotato di uno Sportello d'ascolto e, grazie ai fondi stanziati con il PNRR, ha previsto numerosi corsi di mentoring dedicati sia agli alunni sia alle famiglie. Altresì il Collegio Docenti ha deliberato l'introduzione dall'anno scolastico 2025/2026 di un apposito modulo, allegato al presente documento, che permette la segnalazione dei casi.

4.3 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”, 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.

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.

4.4. Allegati con le procedure da seguire

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. 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.

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 con azioni differenti come ad es. 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, durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

Il nostro piano d'azioni

L'Istituto si propone di informare tutte le componenti scolastiche riguardo i nominativi dei referenti di Istituto e di plesso per il bullismo e cyberbullismo e le procedure per la segnalazione dei casi sia attraverso il sito di istituto sia attraverso iniziative mirate.

Procedure interne: cosa fare in caso di evidenza di Cyberbullismo



Il docente ha evidenza che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Se non è già stato fatto, avvisa il referente per il cyberbullismo (e/o il team antibullismo) che attiva le procedure ("Corso 4" della piattaforma ELISA) e il Dirigente Scolastico.
Ricordare sempre che in base alla legge 71-2017:

- A) Se c'è fattispecie di reato va fatta la segnalazione alle forze dell'ordine
B) Se non c'è fattispecie di reato.

Il DS (e/o il team antibullismo):

- informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto) su quanto accade e condivide informazioni e strategie.
- Informa i genitori di ragazzi/e infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy)
- Attiva il consiglio di classe.

Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

NELLE CLASSI

Il team antibullismo collabora coi docenti della classe per realizzare l'intervento nella classe:

- a seconda della situazione valutata se
- affrontare direttamente l'accaduto o
 - sensibilizzare la classe (vedi Corso 4 Piattaforma Elisa)
 - trova il modo di supportare la vittima e di responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.

A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnala alla Polizia Postale:

a) contenuto; b) modalità di diffusione.

Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



Il docente riceve una segnalazione (da un genitore, un altro studente ...) o sospetta che stia accadendo qualcosa a uno/a studente/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

Condividi con il referente o al team antibullismo: si attiva il processo di attenzione e valutazione a cura del referente.

- Insieme si valuta se è il caso
- di avvisare il consiglio di classe;
 - di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.

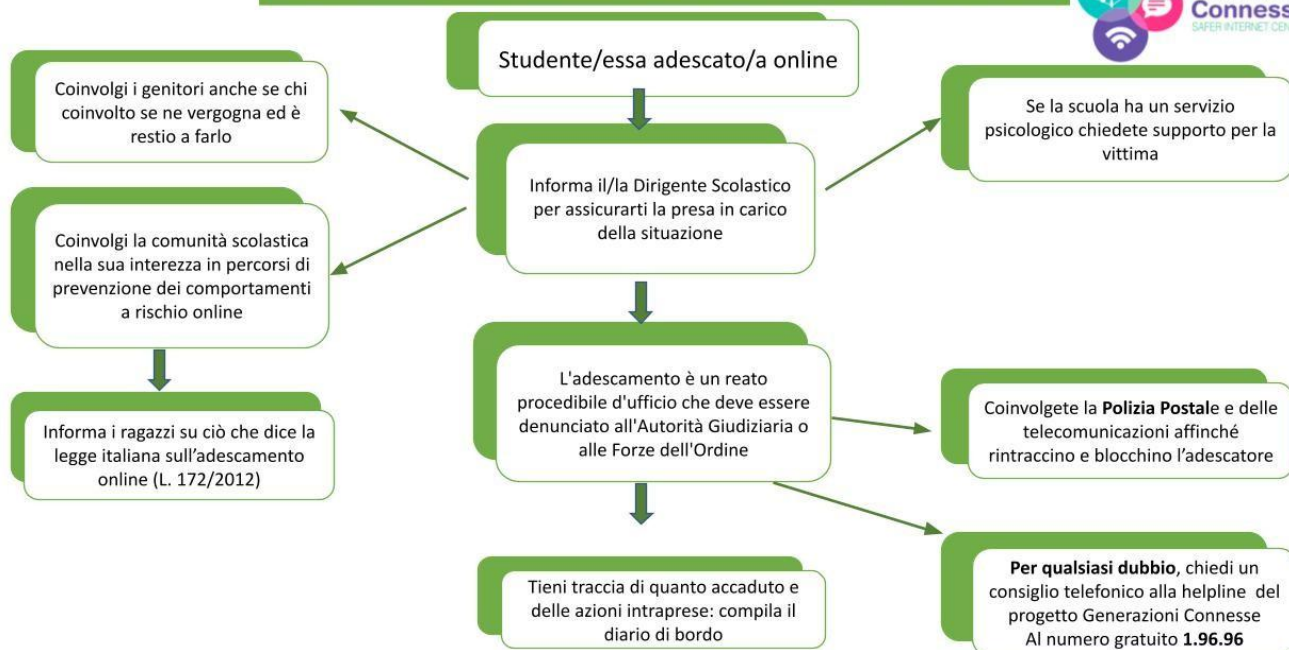
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Scarica le linee di orientamento per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo

Se emergono evidenze passa allo schema successivo

Ricorda a studenti/esse che possono chiedere in qualsiasi momento una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 o via chat

Procedure interne: cosa fare in caso di Adescamento Online?



Procedure interne: cosa fare in caso di diffusione non consensuale di immagini intime?



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

