



Documento di ePolicy

NATF15000E

ITI E. MAJORANA SOMMA VESUVIANA

VIA SAN SOSSIO 7 - 80049 - SOMMA VESUVIANA - NAPOLI (NA)

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

1. Presentazione dell'ePolicy

1. Scopo dell'ePolicy
2. Ruoli e responsabilità
3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
5. Gestione delle infrazioni alla ePolicy
6. Integrazione dell'ePolicy con regolamenti esistenti
7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

2. Formazione e curriculum

1. Curriculum sulle competenze digitali per gli studenti
2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
4. Sensibilizzazione delle famiglie e Patto di corresponsabilità

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

1. Protezione dei dati personali
2. Accesso ad Internet
3. Strumenti di comunicazione online
4. Strumentazione personale

4. Rischi on line: conoscere, prevenire e rilevare

1. Sensibilizzazione e prevenzione
2. Cyberbullismo: che cos'è e come prevenirlo
3. Hate speech: che cos'è e come prevenirlo
4. Dipendenza da Internet e gioco online
5. Sexting
6. Adescamento online
7. Pedopornografia

5. Segnalazione e gestione dei casi

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

Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet. L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse. L'e-policy è un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie digitali positivo, critico e consapevole, sia da parte degli studenti e studentesse che dagli adulti coinvolti nel processo educativo. Questo Documento verrà aggiornato ogni qualvolta si presentano novità in materia digitale e inserito nel PTOF.

1.2 - Ruoli e responsabilità

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

L'Istituto "ITI Ettore Majorana Somma Vesuviana (Na)" ha elaborato questodocumento in conformità con le "Linee di orientamento per azioni di contrasto al bullismo e al cyberbullismo" del 15 aprile 2015, con successiva nota Miur di aggiornamento "Linee di orientamento per la prevenzione del bullismo e del cyberbullismo" di ottobre 2017 e in linea alle "Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente", C189/9, p.9. L'obiettivo è di educare e sensibilizzare gli alunni, gli insegnanti e i genitori all'uso sicuro e consapevole di Internet.

Per la strutturazione del Curricolo sulle competenze digitali, si rinvia alla progettazione dipartimentale.

Infatti lo sviluppo delle Nuove Tecnologie, il loro utilizzo nell'ambito didattico e la maggiore diffusione nella vita di tutti i giorni di questi strumenti, richiede responsabilità e consapevolezza. È compito dell'intera comunità scolastica, genitori

inclusi, garantire che gli studenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato e sicuro. Di qui la necessità di dotare la Scuola di una propria e-Policy di E-safety, per gestire le eventuali infrazioni come integrazione del Regolamento d'Istituto.

1.3 - Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

La scuola propone una formazione finalizzata alla crescita globale del singolo alunno, che tenga presente delle fasi evolutive e quindi atta ad individuare in maniera chiara e inequivocabile ruoli e responsabilità di ciascuno degli attori del percorso formativo.

Il Dirigente Scolastico promuove la formazione consapevole per l'utilizzo della Rete e si impegna a:

- **definire** le linee di indirizzo del P.T.O.F. e del Patto di Corresponsabilità affinché contemplino misure specifiche dedicate alla prevenzione del cyberbullismo, prevedendo all'interno del P.T.O.F,
- **garantire** la corretta formazione del personale scolastico sulle tematiche relative all'uso sicuro e consapevole di Internet e della rete;
- **garantire** una formazione adeguata del personale docente relativo sull'utilizzo

delle TIC nella didattica e l'uso corretto e sicuro di questi strumenti per una sana e proficua navigazione in Rete

- **assicurare** un sistema di monitoraggio e controllo per la sicurezza in Rete, condiviso dall'intera comunità educante e dal personale ATA;
- **garantire** tutte le forme di intervento qualora si verificano atti di bullismo e cyber bullismo, secondo le norme previste;
- **assicurare** che le norme proposte dall'Istituto vengono revisionate e calate nelle situazioni particolari, proponendo soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola.

L'animatore Digitale, per prevenire e controllare il fenomeno, supportato dal Team dell'innovazione, deve:

- **proporre** la formazione interna all'Istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi online e alle misure di prevenzione e gestione degli stessi;
- **rilevare** i problemi relativi all'utilizzo sicuro delle tecnologie digitali e di internet a scuola;
- **controllare** che la scuola sia cablata, per permettere a tutta la comunità scolastica l'accesso alla Rete, muniti di Password applicate e regolarmente cambiate;
- **curare** la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti.

Il Referente del bullismo e cyberbullismo:

- **si premura** di coordinare e promuovere attività specifiche per la prevenzione e il contrasto del bullismo e cyberbullismo e può avvalersi della collaborazione delle Forze di Polizia, nonché Associazioni e Centri di Aggregazione Giovanile presenti sul territorio;
- **organizza** percorsi formativi e progetti individualizzati per alunni, docenti e genitori.
- **denuncia** tempestivamente all'Autorità giudiziaria e/o agli organi competenti atti di bullismo e cyber bullismo;
- **motiva** al monitoraggio l'intera comunità, coinvolgendo in prima persona gli alunni, per renderli consapevoli della gravità di azioni deviate.

Il Direttore dei servizi generali e amministrativi deve:

- **assicurare**, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che le strutture scolastiche siano in sicurezza per evitare attacchi esterni dannosi
- **garantire** una corretta comunicazione interna, attraverso circolari, sito web, ecc., fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di Internet.

I Docenti:

- **hanno il diritto e il dovere** e di informarsi e informare sulle 'utilizzo delle tecnologie digitali e di Internet in sicurezza, rispettando il regolamento e la politica di sicurezza adottata dalla scuola;
- **garantire** che le modalità di utilizzo corretto e sicuro delle TIC e di Internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- assicurarsi che gli alunni facciano un corretto utilizzo della Rete e comprendano e seguano le regole di prevenzione e di contrasto al fenomeno;
- **intraprendono** azioni che favoriscano sia l'acquisizione che il rispetto di regole che creino nella classe "senso di comunità";
- **utilizzano**, nell'attività didattica, tecniche di apprendimento cooperative e di uso delle tecnologie digitali nella didattica;
- **segnalano** tempestivamente al Docente Referente ed al Dirigente scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse;
- **promuovono** la riflessione sulle conseguenze che ogni atto di sopraffazione e intolleranza crea, in primis, per le vittime;
- **intervengono** per proteggere la vittima;
- **inoltrano** con solerzia denuncia all'Autorità giudiziaria e/o agli Organi competenti, qualora gli atti di cyberbullismo si configurino come veri e propri reati perseguibili d'ufficio.

Le Alunne e gli Alunni devono:

- **utilizzare** le TIC in linea alle richieste dei docenti, per essere responsabili, in relazione al proprio grado di maturità e di apprendimento, avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali, ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;
- **sviluppare** un senso di appartenenza alla scuola anche attraverso l'attuazione delle pratiche buone e comprendere l'importanza della sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;
- **adottare** condotte rispettose degli altri anche quando si comunica in rete;
- con il supporto della scuola **imparare a tutelarsi** on-line, a tutelare i propri pari e rispettarli.

Il personale Amministrativo, Tecnico e Ausiliario (ATA)

- **partecipa** a corsi di formazione ed autoformazione in tema di bullismo e cyberbullismo;
- **segnala** al Dirigente scolastico comportamenti non adeguati e/o episodi di bullismo/cyberbullismo;
- **collabora** con il Docente referente nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

I Genitori sono chiamati a:

- **sostenere** la linea di condotta della scuola adottata nei confronti dell'utilizzo delle TIC nella didattica;
- **vigilare** sulla condotta dei ragazzi e sull'uso che fanno delle tecnologie nelle ore extra scolastiche; relazionandosi a riguardo in modo costruttivo con i docenti, qualora i minori non fanno uso responsabile delle TIC.

Gli Enti esterni e le Associazioni devono:

- **conformarsi** alla politica della scuola riguardo l'uso consapevole delle TIC e della Rete;
- **promuovere** comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti durante le attività che si svolgono insieme.

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

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

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

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

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

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

Il Documento E-Policy, approvato dal Collegio dei Docenti e dal Consiglio d'Istituto, viene pubblicato sul sito della scuola e presentato a soggetti esterni che erogano attività educative nell'Istituto. Gli studenti vengono informati del monitoraggio

praticato per la navigazione online, negli spazi della scuola e sulle regole di condotta da tenere in Rete e nelle relazioni. Gli interventi sono supportati dalle Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola messe a disposizione da MIUR-Generazioni Connesse Safer Internet Centre. Il Dirigente scolastico ed al Referente del bullismo/cyberbullismo e/o al referente dell'E-policy verranno forniti di opportuni riferimenti interni per la relativa e tempestiva comunicazione.

1.5 - Gestione delle infrazioni alla ePolicy

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

A seconda dell'età dello studente o della studentessa l'intervento è rivolto al contesto classe con attività specifiche educative, allo scopo di promuovere una maggiore consapevolezza circa l'uso dell TIC e di Internet.

Se l'episodio è considerato grave, è opportuno denunciare alla Polizia Postale o garantire un immediato supporto psicologico agli alunni coinvolti, attraverso i servizi preposti. Il personale scolastico deve essere formato riguardo le infrazioni in Rete.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

Si allegano al presente Documento il Regolamento dell'Istituto scolastico e il Patto di Corresponsabilità pubblicati nel PTOF dell'ITI MAJORANA Somma Vesuviana (Na)

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

Il nostro piano di monitoraggio e di aggiornamento prevede la formazione del gruppo di lavoro E-policy, costituito dal Referente per la prevenzione del bullismo e del cyberbullismo, le dalle Funzioni Strumentali Area 1 (Sostegno ai docenti); Area 2 (Sostegno agli Studenti); Area 4 (Animatore Digitale); Area 5 (PTOF e RAV).

- Si prevede una riunione dei Coordinatori di Dipartimento per discutere delle attività relative all'E policy;
- Realizzazione di un sistema di monitoraggio delle attività di prevenzione e formazione (somministrazione a campione nelle classi prime sulle azioni di prevenzione del bullismo e del cyberbullismo);
- Monitoraggio dell'efficacia dell'E-policy attraverso sondaggio rivolto a tutte le componenti dell'Istituto;
- Formazione del personale docente e non docente sui reati on-line e sulla privacy;
- Revisione del Regolamento d'Istituto.
- Implementazione della dotazione tecnica delle classi, per quanto concerne LIM, PC, tablet (anche in comodato d'uso agli studenti) con particolare attenzione nei confronti degli allievi con BES, nei limiti delle dotazioni finanziarie dell'Istituto e dei fondi dedicati.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

Azioni da svolgere nei prossimi 3 anni:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

Capitolo 2 - Formazione e curriculum

2.1. Curricolo sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più “intuitivo” ed “agile” rispetto agli adulti, ma non per questo sono dotati di maggiori “competenze digitali”.

Infatti, “la competenza digitale presuppone l’interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l’alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l’alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l’essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico” ([“Raccomandazione del Consiglio europeo relativa alla competenze chiave per l’apprendimento permanente”](#), C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curriculum digitale.

La scuola promuove una formazione continua per docenti e studenti, la cui finalità è l’uso consapevole e responsabile delle tecnologie digitali. Si predispongono attività di progettazione e implementazione per l’elaborazione curriculum digitale a cura dei Dipartimenti e dei Consigli di Classe.

2.2 - Formazione dei docenti sull’utilizzo e l’integrazione delle TIC (Tecnologie dell’Informazione e della

Comunicazione) nella didattica

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

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

Da diversi anni l'ITI Majorana fruisce di tecnologie informatiche che via via si sono perfezionate come impone il progresso tecnologico. Attualmente è in uso il registro elettronico, LIM, ambienti di condivisione, tutto finalizzato alla didattica dell'inclusione, non solo in relazione ai Bisogni Educativi Specifici, ma più in generale per facilitare un percorso di apprendimento in grado di promuovere il successo formativo, offrendo risposte adeguate ed efficaci "a tutti e a ciascuno". Tutto ciò nel rispetto della libertà di insegnamento e delle propensioni personali del singolo docente.

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

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

Presso l'ITI Majorana si sta progettando una formazione per i docenti sulle tematiche dell'Inclusione, l'uso consapevole delle TIC. Si sono organizzati convegni e dibattiti con personale esperto, sui rischi online, sul bullismo e sul cyberbullismo. Interventi di prevenzione su queste due ultime tematiche vengono tenuti tutti gli anni alle classi del biennio con la partecipazione dei docenti curricolari. Inoltre la scuola promuove la partecipazione dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto "Generazioni Connesse".

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

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

Le famiglie vengono continuamente informate e sensibilizzate tramite e con i loro figli. Inoltre il sito della scuola rimane un valido strumento per mantenere viva la relazione scuola/famiglie. Tra le attività di coinvolgimento delle famiglie è previsto un sondaggio telematico per i genitori, per rilevare le tematiche di interesse nell'ambito dell'educazione alla cittadinanza digitale e dell'inclusione. A partire dal prossimo anno scolastico, verranno indicate alcune proposte per integrare il Patto di Corresponsabilità, da definire e approvare nelle sedi opportune.

Il nostro Piano D'azione da sviluppare nell'arco dei tre anni scolastici successivi prevede:

- coinvolgimento di una rappresentanza di genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale;
- organizzazione e promozione di incontri formativi per il corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali;
- organizzazione di incontri con esperti sulle competenze digitali, sull'educazione alla cittadinanza digitale.
- prevenzione bullismo e cyberbullismo nella classi prime e seconde;
- prevenzione dei reati on-line nelle classi quinte;
- promozione di percorsi formativi per lo sviluppo delle competenze digitali;
- implementazione della sperimentazione 2.0;
- avvio della fase istruttoria per la redazione della E-policy

Il nostro piano d'azioni

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

- Organizzare incontri con esperti per i docenti sulle competenze digitali.

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

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.
-
-

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

L'ITI Majorana, per l'adempimento alla normativa vigente sulla Privacy, ha dedicato una sezione specifica, reperibile sul sito della scuola già ad inizio anno scolastico, per far pervenire alle famiglie o ai tutor degli alunni, i relativi moduli per l'acquisizione dei consensi, i dati del Dpo, la politica sulla protezione dei dati personali. Inoltre è in uso il registro dei trattamenti e degli accorgimenti tecnici e strutturali finalizzati alla tutela della riservatezza dei dati della intera comunità scolastica.

3.2 - Accesso ad Internet

- 1. L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
- 2. Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
- 3. Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
- 4. L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
- 5. Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

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

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli

studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di “fornire a tutte le scuole le condizioni per l’accesso alla società dell’informazione e fare in modo che il “diritto a Internet” diventi una realtà, a partire dalla scuola”.

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

Il nostro Istituto è dotato di strumenti tecnologici in tutte le aule e i laboratori, finanziati con i fondi del Piano Nazionale Scuola Digitale.

La connessione scolastica è supportata dalla fibra ottica in modalità via cavo e Wi-Fi per garantire tutte le attività didattiche ed amministrative online. La rete amministrativa è diversa da quella didattica grazie a server dedicato con modi e regole diversificate per garantire la sicurezza e la protezione dei dati sensibili.

Il Dirigente Scolastico, il Direttore dei Servizi Generali e Amministrativi ed il personale degli uffici della segreteria hanno account personalizzati e accedono ai servizi tramite pwd adeguate e procedura di autenticazione personale. L’assistenza tecnica del server e delle apparecchiature informatiche è continua e affidata a ditta specializzata esterna che provvede al controllo sul backup dei dati, all’aggiornamento dei sistemi operativi e degli antivirus installati sulle macchine e al controllo del funzionamento del firewall. Tutte le aule del biennio e parte delle aule del triennio sono raggiunte dalla Rete didattica e munite di strumenti multimediali. A breve sarà completata la dotazione di strumenti digitali per le restanti classi. Gli studenti accedono alla rete sotto il controllo dei docenti e degli assistenti durante le attività didattiche. Gli strumenti tecnologici vengono utilizzati per qualsiasi attività inerente alla scuola per cui sia i docenti sia gli studenti adottano le indicazioni previste dai regolamenti approvati dal Consiglio di Istituto circa l’accesso alla Rete e ai dispositivi tecnologici. I regolamenti sono pubblicati sul sito web della scuola.

3.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L’uso degli strumenti di comunicazione online a scuola, al fianco di

quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

La scuola per le comunicazioni adotta il Sito scolastico, costantemente aggiornato e curato dall'animatore digitale, sul quale vengono inserite le notizie e le attività svolte per gli alunni e dagli alunni; attraverso il Registro Elettronico che consente di gestire in modo ottimale la comunicazione con le famiglie che hanno la possibilità di essere costantemente informate, interagendo direttamente con la scuola, dotati di un profilo assegnato dal sistema, per la comunicazione sull'andamento didattico-disciplinare dell'alunno, per la prenotazione dei colloqui e per prendere atto della programmazione didattica. I docenti possono comunicare con le famiglie anche in maniera informale con dispositivi personali, ma ogni contatto viene dettagliatamente protocollato e riportato sul registro elettronico dell'Istituto. La comunicazione formale con le famiglie avviene tramite l'invio dalle mail istituzionale della scuola alle mail personali dei genitori. Attualmente l'unica e condivisa piattaforma utilizzata dalla nostra comunità scolastica è Google Workspace.

3.4 - Strumentazione personale

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

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

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

Per gli studenti

Gli alunni possono utilizzare durante l'orario scolastico gli strumenti personali, come cellulari, tablet ecc. esclusivamente per le attività didattiche, sotto stretto controllo dei docenti in orario; allo stesso tempo agli allievi non è consentito utilizzare i telefoni cellulari per telefonare, filmare o scattare foto durante le attività curricolari.

La connessione ai servizi di internet per la propria strumentazione viene fatta su rete personale. Eccezione sono gli alunni con BES o DSA, per i quali la scuola garantisce il supporto tecnologico idoneo, ma su richiesta dell'interessato.

Per i docenti

Anche per i docenti l'utilizzo di strumentazioni personali è finalizzato esclusivamente per le attività didattiche e per integrare i dispositivi messi a disposizione dalla scuola. Durante il restante orario di servizio è permesso l'uso di portatili, tablet, per attività funzionali all'insegnamento in entrambe le situazioni ed è garantito l'accesso alla rete wifi negli spazi comuni previsti dalla logistica della rete stessa.

Per il personale della scuola

Durante l'orario di servizio al personale scolastico è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare uno o più eventi o attività volti a formare il personale

adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

Scegliere almeno 1 di queste azioni:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli
- studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro

delle tecnologie digitali (cybersecurity)

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

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

4.2 - Cyberbullismo: che cos'è e come prevenirlo

La legge 71/2017 “Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo”, nell’art. 1, comma 2, definisce il cyberbullismo:

“qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d’identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo”.

La stessa legge e le relative **Linee di orientamento per la prevenzione e il contrasto del cyberbullismo** indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di [cyberbullismo](#) e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
 - Ha il compito di coordinare le iniziative di prevenzione e contrasto del [cyberbullismo](#). A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
 - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d’istituto), atti e documenti (PTOF, PdM, Rav).

Il nostro Istituto pone come centrale la prevenzione e la problematica del bullismo e cyberbullismo e in ottemperanza con le “Linee di Orientamento per la prevenzione e contrasto del Cyberbullismo”, l’Istituto si propone di accrescere le capacità di intervento, sia in ottica preventiva, sia di gestione degli episodi già verificatisi; di approfondire ancora meglio la conoscenza delle tecnologie digitali, del funzionamento del web, delle dinamiche dei social network; di coinvolgere diversi attori, con particolare attenzione ai genitori, e alle realtà aggregative territoriali, per garantire la promozione di azioni di prevenzione e contrasto anche in contesti diversi da quello strettamente scolastico; di diffondere e replicare le iniziative su tutto il territorio

provinciale di riferimento, valorizzando le buone prassi già sperimentate; interiorizzare e potenziare le competenze sociali e civiche; di promuovere negli studenti comportamenti empatici e pro sociali; di promuovere negli studenti buone prassi comportamentali; di promuovere la sicurezza in Rete degli studenti, perché acquisiscano le competenze necessarie all'esercizio di una cittadinanza digitale consapevole; di realizzare un'alfabetizzazione emotiva, individuando nell'analfabetismo emotivo, accresciuto dai mezzi tecnologici, la causa prima di atteggiamenti sociali violenti e intenzionali, di natura sia fisica che psicologica; promuovere la costruzione di un ambiente emotivamente sano, perché esso costituisce un terreno fertile per l'apprendimento e la socializzazione; di supportare docenti e famiglie in momenti di difficoltà; riconoscere l'importanza e la necessità del rapporto con l'adulto come guida autorevole.

Intanto durante questo anno scolastico per prevenire, sensibilizzare e contrastare il cyberbullismo, il referente ha organizzato una giornata di approfondimento sulla Sicurezza in Rete, con particolare attenzione al Bullismo telematico, coinvolgendo gli alunni delle classi III e IV, docenti e famiglie, dal titolo "MAJORANA IN SAFETY E SECURITY".

4.3 - Hate speech: che cos'è e come prevenirlo

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

Il nostro Istituto sta progettando per il prossimo anno scolastico attività inerenti a tali problematiche, per promuovere sempre meglio uno stile inclusivo.

4.4 - Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale?

Il comportamento degli allievi viene continuamente monitorato nel nostro Istituto, facendo attenzione ai comportamenti devianti dei giovani della nostra comunità scolastica e promuovendo, attraverso tutte le attività didattiche e con una progettazione per competenze trasversali, in merito alla cittadinanza digitale, al cyberbullismo e ad un uso integrativo e non sostitutivo della Rete; promuovere atteggiamenti sani, scongiuranti la morbosità e dipendenza verso il gioco online o all'abuso di navigazione virtuale impropria. Dei casi negativi registrati, le famiglie vengono tempestivamente informate, proponendo percorsi rieducativi con i docenti di informatica o, nei casi di dipendenza più gravi, il rinvio a personalità competenti. L'istituto promuoverà azioni di prevenzione attraverso percorsi sul benessere digitale.

4.5 - Sexting

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti 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.

La scuola si propone a tale riguardo l'organizzazione di eventi e incontri, con la partecipazione della Polizia Postale per la prevenzione del fenomeno; si propone di organizzare con l'Arma dei Carabinieri per le classi quinte per la prevenzione e la

sensibilizzazione sui reati legati all'utilizzo di internet e delle piattaforme on-line; ci si propone di organizzare progetti e PCTO mirati all'inclusione, all'accettazione e alla valorizzazione della diversità, al dialogo interreligioso e interculturale, alla destrutturazione degli stereotipi, alla prevenzione della violenza di genere.

4.6 - Adescamento online

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

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

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

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

Per il prossimo anno scolastico sono previste attività per prevenire ed affrontare il problema dell'adescamento in Rete. Intanto, durante questo anno scolastico, è stato organizzato un Convegno online per la sicurezza in Rete, tenuta da un Dirigente informatico Ministero della Giustizia, già funzionario della sicurezza presso il MIUR; da una psicologa psicoterapeuta, coordinatrice del Centro antiviolenza Maya e dal Presidente dell'associazione no profit Populorum Progressio.

4.7 - Pedopornografia

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

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

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

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

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

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

Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il “Clicca e Segnala” di [Telefono](#)

Azzurro e "STOP-IT" di Save the Children.

Per questa diffusa e orripilante problematica l'ITI Majorana dal prossimo anno scolastico si propone di attivare opere di sensibilizzazione, rivolta ai genitori e all'intera comunità scolastica, promuovendo i servizi di Generazioni Connesse: il servizio Hotline che 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.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

- 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/le studenti/studentesse, con il coinvolgimento di esperti.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.
- 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/le studenti/studentesse.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.

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

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

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

Scegliere almeno 1 di queste azioni:

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/le studenti/studentesse, con il coinvolgimento di esperti.

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

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

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/le studenti/studentesse.

Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.

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

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



Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di [Helpline 19696](#) e [Chat di Telefono Azzurro](#) per supporto ed emergenze;
- [Clicca e segnala di Telefono Azzurro](#) e [STOP-IT di Save the Children Italia](#) per

segnalare la presenza di materiale pedopornografico online.

Qualora si verifica un qualsiasi spiacevole episodio, o si possa avere il semplice sospetto atti di cyberbullismo, sexting o adescamento online, il personale scolastico nonchè gli enti, associazioni, professionisti esterni alla scuola con i quali si abbiano convenzioni, sono tenuti ad intervenire e denunciare l'accaduto.

5.2. - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

- CASO A (SOSPETTO) – Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.
- CASO B (EVIDENZA) – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

Per tutti i dettagli fate riferimento agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;

- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito [1.96.96](tel:19696).

L'ITI Majorana segnala gli episodi direttamente tramite il Referente del Bullismo e Cyberbullismo, che si rende disponibile personalmente.

5.3. - Gli attori sul territorio

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

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

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

- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale:** supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni:** accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali:** forniscono supporto per le conseguenze a livello
-

psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.

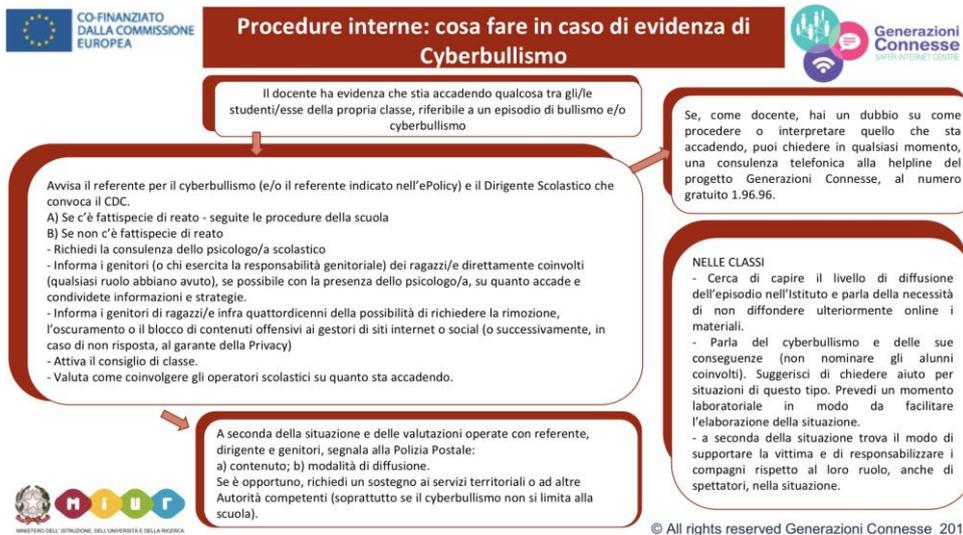
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico:** segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

Se il fenomeno si presenta in forma grave e dovesse dunque richiedere interventi che esulano dalle competenze e possibilità della scuola, è possibile rivolgersi ad enti e servizi presenti sul territorio di cui si forniscono gli opportuni riferimenti:

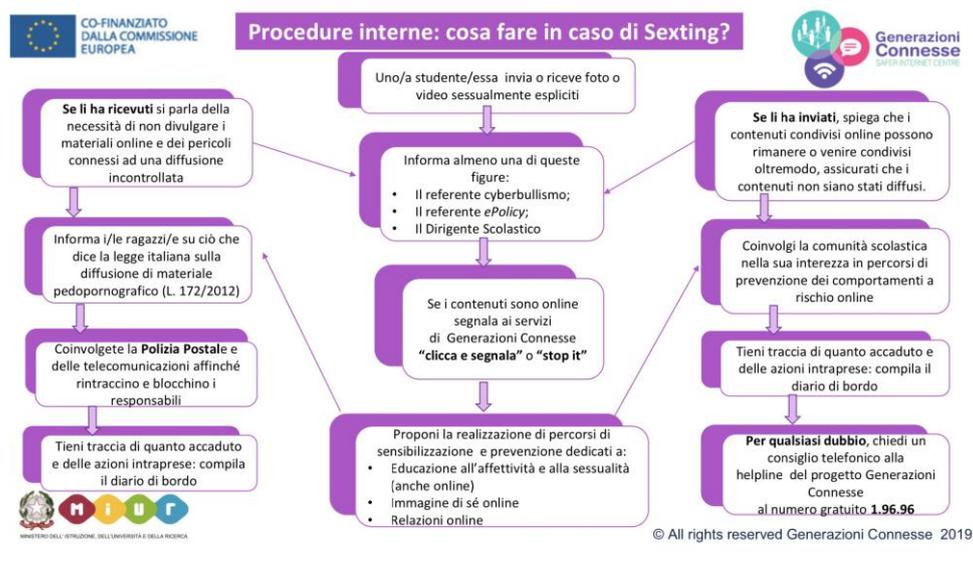
- **Comitato Regionale UNICEF**, Telefono: 081 71 470 57, fax: 081 64 58 95 e-mail: comitato.campania@unicef.it;
- **Ufficio Scolastico Regionale per la Campania** Via Ponte della Maddalena, 55, 80142 Napoli;
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico** www.regione.campania.it;
- **ASL NA 3 Sud**;
- **Tribunale dei Minorenni** Centralino: 0039. 081 7449111, Fax: 0039. 081 7419132, patrocinio.tribmin.napoli@giustizia.it;
- **Polizia postale e delle telecomunicazioni** Via Delle Repubbliche Marinare 497 - 80146 Napoli (NA), cell: 335 1727185

5.4. - Allegati con le procedure

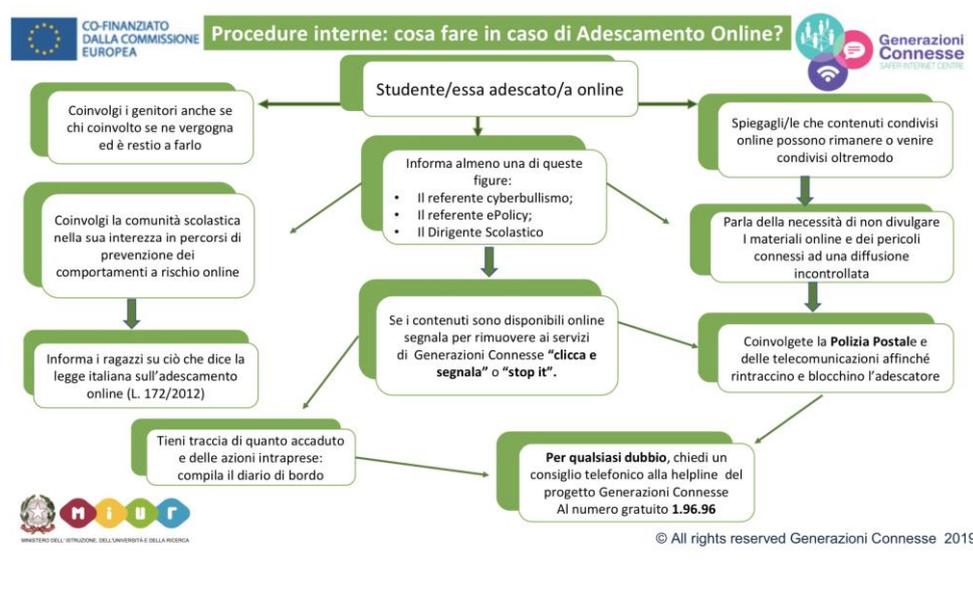
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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

