



Documento di ePolicy

TAEEO8300V

C.D. "MARIA PIA"

VIA QUATTRO NOVEMBRE 1 - 74027 - SAN GIORGIO IONICO - TARANTO (TA)

GIUSEPPE FALANGA

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.

Le nuove sfide sociali emerse in quest'ultimo periodo vanno affrontate attraverso processi nuovi che richiama persone e comunità a nuove responsabilità. In questo cambiamento culturale, la scuola

ha un ruolo centrale di promozione di consapevolezze e di azioni concrete di cittadinanza attiva, anche nella prospettiva di patti educativi territoriali che dovranno concretizzarsi per garantire una riapertura dell'anno scolastico sicura ed inclusiva. Detto ciò, il nostro Circolo Didattico "Maria Pia di Savoia" è una realtà scolastica attestata nel territorio locale come punto di riferimento educativo e culturale, affermata negli anni come "agenzia educativa" in grado di coniugare tradizione e modernità, ponendo al centro delle proprie attenzioni pedagogiche la 'persona' dell'alunno, per formarlo come cittadino consapevole e competente, favorendo l'apprendimento critico delle conoscenze, delle abilità e delle competenze in relazione ai cambiamenti sociali e alle sfide culturali emergenti. Coerentemente alla sua vision, la nostra scuola ha aderito anche per il corrente anno scolastico 2019/2020 per il decimo anno consecutivo, al Progetto "Scuola Amica delle bambine, dei bambini e degli adolescenti", che vede la collaborazione tra l'UNICEF Italia e il Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR). Il progetto, come ben si sa, è finalizzato ad attivare prassi educative volte a promuovere la conoscenza e l'attuazione della Convenzione ONU sui diritti dell'infanzia e dell'adolescenza e il relativo Protocollo attuativo permette al suddetto progetto di essere perfettamente in linea con le indicazioni per l'insegnamento di EDUCAZIONE CIVICA, in cui si evidenzia come l'educazione alla cittadinanza attiva, alla partecipazione e alla cultura della Legalità costituisca parte integrante dell'apprendimento. È importante sottolineare il valore che il Progetto Scuola Amica assume anche nell'ambito delle attività di prevenzione delle diverse forme di esclusione, discriminazione, bullismo e cyberbullismo, in linea con la legge n. 71 del 29 maggio 2017, "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", che intende contrastare questo fenomeno in tutte le sue manifestazioni, con azioni a carattere preventivo e con una strategia di attenzione, tutela ed educazione nei confronti di tutti i minorenni coinvolti. Anche tutte le attività inerenti al PNSD, regolarmente incluso nel nostro PTOF, mirano allo sviluppo di competenze digitali e sociali coerentemente con le indicazioni fornite dal MIUR. Inoltre, la fruibilità gratuita di uno Sportello di Ascolto, con la finalità di contribuire a migliorare la qualità della vita scolastica, facilitando il dialogo e la costruzione di rapporti positivi tra docenti, alunni e genitori, e l'adesione della nostra scuola da anni al progetto di GENERAZIONI CONNESSE, contribuiscono ad orientare la nostra scuola alla valorizzazione e alla cura di relazioni di prossimità aperte all'alterità, nonché alla sollecitazione di idee e scelte ispirate ai valori di Giustizia e Pace.

Ciò premesso, munire la nostra scuola anche di un documento programmatico, qual è l'ePolicy, specifico sia nell'indicazione di un proprio codice di condotta nella prevenzione e gestione dei casi di cyberbullismo sia nell'indicazione di un regolamento di sicurezza informatica, è per la nostra comunità educante un'occasione imperdibile per educare e sensibilizzare in maniera più incisiva e puntuale alunni, insegnanti e genitori all'uso sicuro e consapevole della Rete, ancor più, a nostro avviso, essendo noi operatori nella fascia della scuola Primaria, dovel'azione di prevenzione costituisce un valore aggiunto.

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.

Si indicano qui di seguito ruoli, compiti e responsabilità di ciascuna delle figure professionali che, a vario titolo, si occupano di gestione e programmazione delle attività formative, didattiche ed educative dell'Istituto e di tutte quelle figure appartenenti alla comunità educante:

IL DIRIGENTE SCOLASTICO

- Garantire la sicurezza, anche online, di tutti i membri della comunità scolastica, in conformità al quadro formativo di riferimento e alle indicazioni del MIUR;
- Promuovere la cultura della sicurezza online, dando il proprio contributo, in concertazione con il docente referente, di corsi di formazione specifici sull'utilizzo positivo e responsabile delle TIC;
- gestire ed, eventualmente, intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

L'ANIMATORE DIGITALE

- stimolare la formazione interna alla scuola negli ambiti del PNSD, attraverso l'organizzazione di laboratori formativi, favorendo l'animazione e la partecipazione di tutta la comunità scolastica alle attività formative;
- Coinvolgere la comunità scolastica, favorendo la partecipazione e stimolando il protagonismo degli studenti nell'organizzazione di workshop e altre attività, anche strutturate, sui temi del PNSD, anche attraverso momenti formativi aperti alle famiglie e ai docenti, per la realizzazione di una cultura digitale condivisa;
- individuare soluzioni metodologiche e tecnologiche sostenibili da diffondere all'interno degli ambienti della scuola (es. uso di particolari strumenti per la didattica di cui la scuola si è dotata; adozione di metodologie comuni;
- informare su innovazioni tecnologiche e laboratoriali, come il coding, per tutti gli studenti, coerenti con l'analisi dei fabbisogni della scuola stessa, anche in sinergia con attività di assistenza tecnica condotta da altre figure.

IL REFERENTE BULLISMO E CYBERBULLISMO

- coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e il cyberbullismo, avvalendosi anche della collaborazione delle Forze di Polizia e delle associazioni del territorio;
- coinvolgere con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.

I DOCENTI

- diffondere la cultura dell'uso responsabile delle TIC e della Rete, integrando parti del curriculum della propria disciplina con approfondimenti ad hoc, ma anche promuovendo,

laddove possibile, l'uso delle tecnologie digitali nella didattica;

- segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che veda coinvolti alunni e alunne.

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

- essere coinvolti nella segnalazione di comportamenti non adeguati e/o di episodi di bullismo /cyberbullismo, raccogliendo, verificando e valutando le informazioni inerenti a possibili casi di bullismo/cyberbullismo.

GLI ALUNNI E LE ALUNNE

- utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti, naturalmente, in relazione alla consapevolezza raggiunta;
- imparare a tutelarsi online, ma anche a tutelare e a rispettare i propri compagni e le proprie compagne;
- partecipare attivamente a progetti e attività che riguardano l'uso positivo delle TIC e della Rete, facendosi anche promotori di quanto appreso attraverso possibili percorsi di peer education.

I GENITORI

- essere partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, ma anche sull'uso responsabile dei device personali;
- relazionarsi in modo costruttivo con i docenti sulle linee educative riguardanti TIC e Rete;
- comunicare ai docenti eventuali problemi rilevati nei propri figli in riferimento ad un uso irresponsabile delle tecnologie digitali o di Internet;
- accettare e condividere quanto scritto nell'ePolicy dell'Istituto.

Per un approfondimento sui ruoli e le responsabilità delle figure presenti a scuola: Legge 59/97, Art. 21 CO° 8; Legge N.165/2001 Art. 25; CCNL; DPR n. 275/99; Legge n.107/2015; Piano Nazionale Scuola Digitale.

In merito alle diverse responsabilità nel percorso di crescita degli studenti e delle studentesse, bisogna ricordare che esiste una corresponsabilità educativa e formativa che riguarda sia i genitori sia la scuola.

In particolare, il 2° comma dell'art. 2048 c.c. così recita: *"I precettori e coloro che insegnano un mestiere o un'arte sono responsabili del danno cagionato dal fatto illecito dei loro allievi e apprendisti nel tempo in cui sono sotto la loro vigilanza"*. Per i genitori, invece, bisogna considerare: il 1° comma dell'art. 30 della Costituzione *"è dovere e diritto dei genitori mantenere, istruire ed*

educare i figli, anche se nati fuori del matrimonio”; il 1° comma dell’art. 2048 c.c. ai sensi del quale “il padre e la madre o il tutore sono responsabili del danno cagionato dal fatto illecito dei figli minori non emancipati o delle persone soggette alla tutela, che abitano con essi (...)”; l’art. 147 del c.c. “l’obbligo di mantenere, istruire, educare e assistere moralmente i figli, nel rispetto delle loro capacità, inclinazioni naturali e aspirazioni (...)”.

Dato questo quadro normativo, rispetto ad un profilo prettamente processuale anche in materia di bullismo e cyberbullismo (dunque non in via esclusiva), si può parlare di **tre tipologie di “culpa”**:

- **culpa in vigilando:** concerne la mancata sorveglianza attiva da parte del docente responsabile verso il minore (così come da art. 2048 del c.c.). Tale condizione è superabile se ci si avvale di una prova liberatoria di non aver potuto impedire il fatto (recita il terzo comma dell’art. 2048 c.c.: “le persone indicate nei commi precedenti sono liberate dalla responsabilità soltanto se provano di non aver potuto impedire il fatto”).
- **culpa in organizzando:** si riferisce ai provvedimenti previsti e presi dal Dirigente Scolastico ritenuti come non soddisfacenti e quindi elemento favorevole al verificarsi dell’eventuale incidente.
- **culpa in educando:** fa capo ai genitori i quali hanno instaurato una relazione educativa con il/la figlio/a, ritenuta come non adeguata, insufficiente o comunque carente tale da metterlo/a nella situazione di poter recare danno a terzi.

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

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

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

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

Per garantire la tutela di studenti e studentesse, torna utile individuare un insieme di regole o norme di comportamento da condividere con organizzazioni/associazioni extrascolastiche ed esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve e/o lungo periodo.

La dirigenza, le figure referenti nei vari ambiti in maniera condivisa con i docenti possono redigere un'informativa ad hoc, salvaguardando i seguenti punti:

- Premessa e obiettivi dell'informativa.
 - Destinatari (organizzazioni e soggetti esterni).
 - Ambiti di applicazione (il progetto specifico o delle attività) e Ruoli (individuare i docenti di riferimento del progetto specifico o delle attività).
 - Regolamento / Codice di comportamento.
 - Procedure di segnalazione (Allegare i moduli di segnalazione per le situazioni di rischio (vedi cap.5 - procedure per soggetti esterni).
 - Provvedimenti nel caso di:
 - omessa segnalazione
 - comportamenti in violazione del codice di comportamento.
-

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

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

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

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

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

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

Nello specifico, l'ePolicy deve essere condiviso e comunicato:

- **agli studenti e alle studentesse** per dare loro regole condivise di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici e per dare loro elementi per poter riconoscere e quindi prevenire comportamenti a rischio sia personali sia dei propri compagni e delle proprie compagne;
- **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;
- **ai genitori**, sul sito istituzionale della scuola, in momenti specifici di formazione e durante gli incontri scuola-famiglia.

Nella comunicazione e condivisione dell'ePolicy è importante valutare i vari target di riferimento (studenti/studentesse, docenti, genitori, personale amministrativo, collaboratori scolastici etc.) individuando di conseguenza i linguaggi, le modalità e i canali di comunicazione e condivisione più adatti. Redigere una versione child friendly del documento per la comunicazione e la sensibilizzazione ai bambini/e è, infatti, di fondamentale importanza per un'adeguata comprensione.

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, è molto importante intervenire su tutto il contesto classe con attività specifiche educative e di sensibilizzazione, allo scopo di promuovere una maggior consapevolezza circa l'utilizzo delle TIC e di Internet.

Le possibili condotte sanzionabili, in relazione all'uso improprio delle TIC e della Rete a scuola da parte degli studenti e delle studentesse, sono:

- la condivisione online di immagini o video di compagni/e senza il loro consenso o che li ritraggono in pose offensive e denigratorie;
- la condivisione di scatti intimi e a sfondo sessuale;
- la condivisione di dati personali;
- l'invio di immagini o video volti all'esclusione di compagni/e.

È opportuno, inoltre, valutare la natura e la gravità di quanto accaduto, al fine di considerare la necessità di denunciare l'episodio (con il coinvolgimento ad es. della Polizia Postale) o di garantire immediato supporto psicologico allo studente o alla studentessa attraverso i servizi predisposti, qualora ciò fosse necessario.

La gestione delle infrazioni riguarda anche il personale scolastico, nel caso in cui i docenti utilizzino impropriamente i device o la Rete o incorrano in violazioni qualora non intervengano nella segnalazione di condotte improprie dei propri studenti e delle proprie studentesse.

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.

Una volta terminata l'ePolicy, verrà allegata ai vari regolamenti scolastici che a loro volta verranno aggiornati alla luce del documento redatto, ne conseguirà relativo inserimento nel PTOF d'Istituto.

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.

Per procedere all'aggiornamento dell'ePolicy, monitorandone le sue azioni, il Dirigente Scolastico provvederà a nominare un referente al quale sarà affidato il compito di revisione dello stesso.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto

ai docenti

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 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.

Per progettare un curriculum sulle competenze digitali bisogna richiamarsi a diverse dimensioni sulle quali sarà possibile lavorare in classe:

- Dimensione tecnologica (importante per far riflettere i più giovani sul potenziale delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana, onde evitare automatismi che abbiano conseguenze incerte, attraverso un'adeguata comprensione della "grammatica" dello strumento):
 1. Riconoscere le criticità tecnologiche e le interfacce;
 2. Selezionare la tecnologia adeguata per ciascun compito;
 3. Operare logicamente;
 4. Rappresentare semplici processi simbolici;
 5. Distinguere tra reale e virtuale.

- Dimensione cognitiva (che fa riferimento alla capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità):
 1. Saper trattare (sintetizzare, rappresentare, analizzare) semplici i testi, i dati, le tabelle e i grafici;
 2. Saper valutare la pertinenza dell'informazione e la sua affidabilità.
- Dimensione etica e sociale (fa riferimento, la prima, alla capacità di gestire in modo sicuro i propri dati personali e quelli altrui, e di usare le tecnologie digitali per scopi eticamente accettabili e nel rispetto degli altri. La seconda, invece, pone un po' più l'accento sulle pratiche sociali e quindi sullo sviluppo di particolari abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di coloro con cui comunichiamo online):
 1. Conoscere i concetti di tutela della privacy;
 2. Rispettare i diritti intellettuali dei materiali reperiti in internet e l'immagine degli altri (la lotta al cyber bullismo un obiettivo importante di questa dimensione);
 3. Comprendere il dislivello sociale e tecnologico che può esistere tra Paesi, persone, generazioni e il problema dell'accessibilità.
- Obiettivo comune alle tre dimensioni:

Sapere comprendere il potenziale delle tecnologie di networking per costruire una conoscenza collaborativa.

Si allegano le rubriche di valutazione:

<https://drive.google.com/file/d/1xQiTRxhBogv1uGEBBo3frhEfiRhDbrxZ/view?usp=sharing>

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.

Le attività di formazione si svolgeranno su due livelli:

1. Formazione istituzionale, organizzata dal MIUR secondo il PNSD, attraverso gli snodi

formativi;

2. Formazione specifica d'istituto, legata alle esigenze formative rilevate a inizio anno a cura dell'animatore digitale, come da progetto incluso nel PTOF.

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

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

Al fine di promuovere la condivisione di buone pratiche per un uso consapevole e sicuro delle ICT, e di prevenire e contrastare "ogni forma di discriminazione e di bullismo, anche informatico" (legge 107/2015, art. 1, c. 7, l), il nostro circolo ha aderito al progetto "Generazioni Connesse" coordinato dal MIUR, in partenariato col Ministero dell'Interno - Polizia Postale e delle Comunicazioni e con altre importanti associazioni per la tutela dei diritti dei minori, come Children Italia e Telefono Azzurro.

L'adesione al suddetto progetto è inserito all'interno del PTOF, con periodo di riferimento dal 2019/20 al 2021/22.

Inoltre, già da alcuni anni, il nostro circolo ha avviato alcune attività:

1. Analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica;
2. Promozione della partecipazione del corpo docente a corsi di formazione sull'utilizzo e l'integrazione delle TIC nella didattica;
3. Organizzazione d'incontri con esperti esterni, Enti e associazioni.

2.4. - Sensibilizzazione delle famiglie e

integrazioni al Patto di Corresponsabilità

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

La nostra scuola ha organizzato già negli anni passati incontri aperti alle famiglie con Enti esterni (come la Polizia Postale, esperti della scuola ecc.) per sensibilizzare docenti, genitori e alunni sui temi della sicurezza online.

Aggiornare il "Patto di corresponsabilità" con specifici riferimenti all'uso delle tecnologie digitali e all'ePolicy è fondamentale, quindi, per informare e rendere partecipi le famiglie sul percorso che volete intraprendere con il documento e il piano d'azione.

È importante, infatti, informare i genitori sulle condotte che si dovranno adottare a scuola e, in generale, offrire loro consigli da mettere in pratica con i propri figli.

A tale scopo la scuola s'impegna a fornire le seguenti azioni d'intervento sull'uso consapevole della Rete:

- **elaborare regole sull'uso delle tecnologie digitali** da parte dei genitori nelle comunicazioni con la scuola e con i docenti (es. mail, gruppo whatsapp, sito della scuola etc.) e informarli adeguatamente anche riguardo alle regole per gli studenti e le studentesse;
 - **fornire ai genitori consigli o linee guida sull'uso delle tecnologie digitali nella comunicazione** con i figli e in generale in famiglia (ad es. a tal fine si potrà fare riferimento alla sezione dedicata ai genitori del sito www.generazioniconnesse.it e fare un richiamo ad essa anche sul sito web della scuola);
 - **organizzare percorsi di sensibilizzazione e formazione dei genitori** su un uso responsabile e costruttivo della Rete in famiglia e a scuola.
 - **prevedere azioni e strategie per il coinvolgimento delle famiglie** in tali percorsi di sensibilizzazione, ad esempio, mediante l'organizzazione di iniziative in cui anche gli studenti e le studentesse siano protagonisti.
-

Il nostro piano d'azioni

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

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.
- 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.

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.

In materia di protezione dei dati personali, si riporta qui di seguito quanto viene esplicitato nella nota M.I. n.388 del 17/03/2020 al paragrafo "La questione privacy":

"Occorre subito precisare che le istituzioni scolastiche non devono richiedere il consenso per effettuare il trattamento dei dati personali (già rilasciato al momento dell'iscrizione) connessi allo svolgimento del loro compito istituzionale, quale la didattica, sia pure in modalità "virtuale" e non nell'ambiente fisico della classe, è.

Le istituzioni scolastiche sono invece tenute, qualora non lo abbiano già fatto, ad informare gli interessati del trattamento secondo quanto previsto dagli artt. 13 e 14 del Regolamento UE 2016/679 e:

- a garantire che i dati personali siano trattati in modo lecito, corretto e trasparente, che siano raccolti per finalità determinate, esplicite e legittime, che siano trattati in modo non incompatibile con tali finalità, evitando qualsiasi forma di profilazione, nonché di diffusione e comunicazione dei dati personali raccolti a tal fine, che essi siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono trattati, e trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
- a stipulare contratti o atti di individuazione del responsabile del trattamento ai sensi dell'articolo 28 del Regolamento, che per conto delle stesse tratta i dati personali necessari per l'attivazione della modalità didattica a distanza;
- a sottoporre i trattamenti dei dati personali coinvolti a valutazione di impatto ai sensi dell'articolo 35 del regolamento."

Ciò detto, in ottemperanza al succitato Regolamento UE 2016/679 e ai Decreti emanati con l'evolversi dell'emergenza sanitaria, ai sensi del D. L. n. 18 del 17/03/2020, il Dirigente scolastico ha provveduto a reclutare un Responsabile della Protezione dei dati personali (RDP o DPO, in inglese - Data Protection Officer) che svolgerà anche attività di assistenza e formazione sugli adempimenti necessari per l'adeguamento alle disposizioni, secondo quanto previsto dal RGPD.

In conformità, quindi, agli obblighi previsti per la normativa vigente sul rispetto della privacy e sul trattamento dei dati personali, il nostro Circolo Didattico ha pubblicato, sul proprio sito web istituzionale, il "Regolamento sulla pubblicazione delle foto e dei video degli studenti afferenti alle attività didattiche ed educative" approvato dal Consiglio di Istituto con delibera n.1 del 3/04/2020, nonché altri documenti informativi destinati a:

-Studenti e Famiglie

-Personale

-Fornitori

Allegati GDPR:

[GDPR - Informativa agli studenti e alle famiglie sul trattamento dei dati personali.pdf](#)

[GDPR - Informativa agli studenti e alle famiglie sul trattamento dei dati personali.pdf](#)

[GDPR - Informativa al Personale sul trattamento dei dati personali.pdf](#)

[GDPR - Informativa ai Fornitori sul trattamento dei dati personali.pdf](#)

Garante per la protezione dei dati personali

<https://www.garanteprivacy.it/regolamentoue/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali>

APPROFONDIMENTO:

“Linee-guida DaD” d’istituto

Movendo dagli esiti della sperimentazione digitale indotta dalla Didattica a Distanza nella gestione emergenziale delle attività scolastiche causata dal Covid-19 nell’a. s. 2019/2020 ed in attuazione della Delibera n. 10 del Collegio dei Docenti del 18 maggio 2020 – nel rispetto delle disposizioni ministeriali sull’impiego delle modalità di interazione telematica in ambito didattico – il Circolo Didattico “Maria Pia” di San Giorgio Jonico intende definire delle Linee-guida che aiutino i docenti, gli alunni e le famiglie a considerare in modo organico ed unitario le potenzialità e le criticità della metodologia DaD nei processi di insegnamento e di apprendimento. Il fine dell’iniziativa è diffondere la consapevolezza sui limiti e sulle opportunità della Didattica a Distanza, garantendo omogeneità di attuazione e regolamentazione nelle classi e nelle sezioni, nel tentativo di assicurare proficua continuità di stimoli e mediazioni ai processi didattico-educativi volti all’ampliamento delle competenze digitali.

In coerenza con le indicazioni ministeriali relative all’eventuale attivazione di processi didattici in area DaD anche nell’a. s. 2020/2021, nell’attesa che siano fornite le Linee guida per la Didattica digitale integrata e data l’incertezza degli scenari e delle procedure gestionali con riferimento anche al fronte della sicurezza, si è convinti che una riflessione estesa ed approfondita su “ciò che è stato” può aiutare a riscoprire le applicazioni digitali della didattica quale risorsa opzionale di crescita professionale per i docenti ed occasione ulteriore di esercizio del diritto all’istruzione per ciascun alunno. Per favorire un organico ed unitario svolgimento delle attività didattiche a distanza, nonché favorire una conduzione ordinata e condivisa delle stesse, i docenti della Scuola dell’Infanzia e della Scuola Primaria saranno chiamati ad elaborare indirizzi elaborati dal Dirigente scolastico con il prezioso ausilio dello Staff DaD, quale contributo offerto al Collegio dei Docenti in termini di orientamento e sollecitazione, nell’ottica di un promettente miglioramento scolastico e professionale. Di seguito è stato predisposto un format essenziale da adottare come matrice di lavoro su cui procedere agilmente alla stesura del Documento, cogliendo anche suggerimenti (relativi ad attività da svolgersi nella Scuola dell’Infanzia e Scuola Primaria) estratti dalla Mini-guida MI-AGIA “Didattica a distanza e diritti degli studenti” del 6 aprile 2020 elaborata dal Ministero dell’Istruzione e dall’Autorità garante per l’infanzia e l’adolescenza, già sottoposte all’attenzione degli insegnanti con Circ. interna n. 226 del 10 aprile 2020. La conclusione del lavoro redazionale è

fissata entro la prima decade del mese di settembre 2020.

3.2 - Accesso ad Internet

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

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

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

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

L'accesso a internet è possibile in tutti i plessi. Nei laboratori di informatica e nelle aule sono attivi

filtri per la navigazione sicura, tramite gestione di blacklist, ed è prevista l'attivazione di software per la gestione e il controllo delle postazioni. Le impostazioni sono definite e mantenute dall'Animatore digitale ed è in carico a ciascun docente la segnalazione di malfunzionamenti e disservizi. I docenti hanno piena autonomia nel collegamento ai siti web nelle postazioni a loro riservate.

1. Gli studenti con certificazione con DSA possono anche utilizzare i propri dispositivi (computer portatile, tablet, e-reader).
2. Non sono ammessi a scuola i videogiochi e vanno segnalati all'insegnante eventuali dispositivi dotati di connessione dati personale.
3. È vietato agli studenti usare dispositivi di registrazione audio, videocamere o fotocamere per registrare video o scattare foto in classe senza il permesso dell'insegnante e senza il consenso della persona che viene registrata o ripresa.
4. Per l'utilizzo dei dispositivi personali degli studenti con DSA viene utilizzata la connessione wifi dell'Istituto. L'accesso alla rete wifi da parte degli studenti attraverso il device di proprietà viene abilitato dal docente responsabile dell'attività al momento dell'inizio della stessa. La connessione viene disabilitata dal docente al termine dell'attività programmata. In nessun caso è consentito agli studenti l'uso della connessione dati personale.
5. Eventuali audio e video registrati a scuola a fini didattici sono realizzati sotto la responsabilità e la stretta sorveglianza degli insegnanti.
6. Agli studenti non è permesso usare i propri dispositivi smart al di fuori dell'orario di lezione come ad esempio pause, uscite didattiche, visite guidate, viaggi d'istruzione, attività facoltative extracurricolari, manifestazioni sportive, spettacoli teatrali ecc.
7. Gli studenti sono responsabili personalmente dei dispositivi portati a scuola e devono custodirli con cura e attenzione. La scuola non risponde di eventuali furti o smarrimenti.
8. La scuola non è responsabile della custodia dei dispositivi e di eventuali danni ad essi cagionati dal proprietario o da altri studenti.
10. Agli studenti è vietato:
 - a. Usare Internet per scopi diversi da quelli didattici;
 - b. Scaricare musica, video e programmi da Internet o qualsiasi file senza il consenso dell'insegnante;
 - c. Utilizzare i social network;
 - d. Giocare sul computer, in rete o offline (a meno che il gioco non faccia parte di una lezione e sia supervisionato dall'insegnante);

e. Utilizzare la Rete e i social network per deridere, offendere, denigrare compagni, docenti, personale scolastico, parenti/amici dei compagni sia in orario scolastico sia in orario extrascolastico.

Si ricorda che, come regolamentato dalle legge 71/2017 (<https://www.gazzettaufficiale.it/eli/id/2017/06/3/17G00085/sg>), la condotta di Cyberbullismo è perseguibile penalmente e qualsiasi atto degli studenti riconducibile a tale fenomeno verrà segnalato (attraverso apposito modello di segnalazione allegato al presente Documento) al Dirigente Scolastico e, successivamente, alle forze dell'ordine.

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.

Gli strumenti di comunicazione on line favoriscono il superamento delle barriere spazio-temporali grazie all'uso di un linguaggio multimediale che punta a promuovere la partecipazione e il coinvolgimento di tutti i soggetti della comunità educante.

Diversi strumenti di comunicazione on line possono essere utilizzati dalla scuola sia per raggiungere target esterni, al fine di valorizzare e promuovere le attività portate avanti dall'istituto, sia per far circolare all'interno della scuola informazioni di servizio o contenuti importanti tra i diversi attori scolastici.

L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. Le credenziali sono in possesso del personale amministrativo. I docenti utilizzano per scopi didattici il proprio account su dominio istruzione.it. La posta elettronica è protetta da antivirus e da antispam.

La scuola ha un sito web e utilizza come registro elettronico "Argo". Tutti i contenuti del settore didattico sono pubblicati direttamente dal referente del sito-web sotto supervisione del Dirigente scolastico che ne controlla la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy. Attualmente nella didattica non si utilizzano social network, neanche da parte dell'istituzione scolastica, e il personale scolastico non è autorizzato a utilizzarli per nome e per conto della stessa.

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: gestione degli strumenti personali - cellulari, tablet, ecc.

a) Salvo casi del tutto eccezionali, i telefoni cellulari non devono essere portati a scuola e non devono comunque essere utilizzati durante l'orario scolastico. Se - malgrado il divieto appena espresso - gli studenti verranno sorpresi ad usare il cellulare, lo stesso verrà temporaneamente requisito dai docenti che registreranno l'episodio sul registro di classe e - in collaborazione con il personale ausiliario e/o con la segreteria - convocheranno per le vie brevi i genitori interessati ai quali verrà riconsegnato il cellulare requisito.

b) L'Istituzione Scolastica non ha e comunque non si assume alcuna responsabilità né relativamente all'uso improprio o pericoloso che gli studenti dovessero fare del cellulare (es.: inviare/ricevere messaggi a/dai soggetti ignoti agli stessi genitori), né relativamente a smarrimenti e/o 'sparizioni' di telefonini cellulari o di lettori mp3 o di hard/disk portatili o pen drive .

c) In ogni caso, i Sigg. genitori tengano conto che le comunicazioni urgenti ed improcrastinabili possono essere trasmesse ai loro figli durante l'orario scolastico rivolgendosi telefonicamente alle singole sedi scolastiche ovvero in Segreteria.

Per i docenti: gestione degli strumenti personali - cellulari, tablet, ecc. Durante le ore di lezione è consentito ai docenti l'uso di dispositivi elettronici personali, come il tablet, unicamente a scopo didattico e a integrazione dei dispositivi scolastici disponibili (il computer di classe), in special modo per l'utilizzo del registro elettronico. Durante il restante orario di servizio l'uso del cellulare è consentito solo per comunicazioni personali che rivestano carattere di urgenza, mentre l'uso di altri dispositivi elettronici personali è permesso per attività funzionali all'insegnamento.

Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet, ecc. Durante l'orario di servizio al restante personale scolastico l'uso del cellulare è consentito per comunicazioni personali urgenti. L'uso di altri dispositivi elettronici personali è permesso solo per attività

funzionali al servizio, e preventivamente autorizzato.

Il nostro piano d'azioni

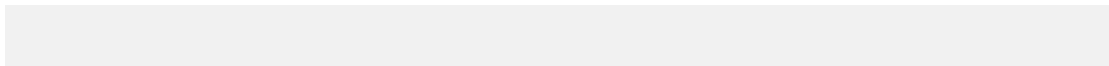
AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse del Circolo 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:

- 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 del Circolo 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 del Circolo 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.

La prima responsabilità degli insegnanti consiste, dunque, nell'imparare a riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente. Tra questi, un'attenzione specifica andrà prestata ai fenomeni di bullismo/cyberbullismo - una forma di prepotenza virtuale attuata attraverso l'uso di internet e delle tecnologie digitali -; sexting - pratica di inviare o postare messaggi di testo e immagini a sfondo sessuale, come foto di nudo o semi-nudo, via cellulare o tramite Internet (Levick& Moon 2010) - e adescamento o grooming - una tecnica di manipolazione psicologica, che gli adulti potenzialmente abusanti utilizzano online, per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata (Glossario di "Generazioni connesse").

L'obiettivo che l'insegnante deve proporsi dopo avere riconosciuto il pericolo è agire di conseguenza, con azioni di contrasto efficaci e mirate.

Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli studenti in orario scolastico, vi sono le seguenti:

- Diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web, condividendo materiali messi a disposizione sul sito del progetto "Generazioni connesse";
- Richiedere di volta in volta autorizzazione esplicita da parte dei genitori all'utilizzo dei dati personali degli alunni (es. liberatoria per la pubblicazione di foto, immagini, video relativi al proprio/a figlio/a per la partecipazione a progetti didattici e altro);
- Far rispettare il divieto di utilizzo di dispositivi digitali propri, quali cellulare e smartphone, agli studenti in orario scolastico. Le dovute eccezioni (uso del cellulare per comunicazioni alunno-famiglia in occasione di uscite didattiche) andranno espressamente regolamentate e dovranno comunque avvenire sotto la supervisione diretta di un docente responsabile;
- Dotare i dispositivi della scuola di filtri che impediscano l'accesso a siti web non adatti ai minori (Blacklist)

Azioni utili a impedire un utilizzo incauto, scorretto o criminoso degli strumenti digitali – materiali inviati, scaricati, ricevuti o condivisi – su dispositivi digitali in uso a scuola (principalmente pc) sono:

- Bloccare l'accesso a un sito o a un insieme di pagine impedendone la consultazione
- Controllare periodicamente i siti visitati dagli alunni
- Utilizzare un software in grado di intercettare le richieste di collegamento e di respingere quelle non conformi alle regole stabilite dall'amministratore
- Affidare a un gruppo di docenti scelto le regole di filtraggio

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).

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

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

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

disabilità, eccetera) ai danni di una persona o di un gruppo.

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

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

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

Da implementare con le indicazioni contenute nella lezione.

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 nostro Circolo, pur riconoscendo la validità delle tecnologie digitali come valido strumento compensativo, intende intraprendere una linea condivisa con la famiglia per stabilire mezzi e modalità durante lo studio domestico, con tempi stabiliti e controllo attivo durante la navigazione in Rete.

4.5 - Sexting

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti mediali sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

Da implementare con le indicazioni contenute nella lezione.

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.

La scuola attiva seminari brevi di formazione, al fine di informare ed accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità; questo per aiutarli ad essere più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri.

Inoltre, all'interno dell'Istituto è presente un docente-tutor (Sportello di Ascolto), con il compito di supportare pedagogicamente gli studenti e le studentesse in difficoltà.

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](#).

Da implementare con le indicazioni contenute nella lezione.

Il nostro piano d'azioni

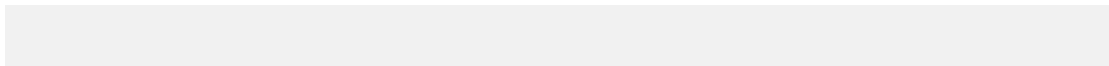
AZIONI (da sviluppare nell’arco dell’anno scolastico 2019/2020).

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.
- ☐ Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- ☐ 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/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 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.



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 minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting:** nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

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

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di [Helpline 19696](#) e [Chat di Telefono Azzurro](#) per supporto ed emergenze;
- [Clicca e segnala di Telefono Azzurro](#) e [STOP-IT di Save the Children Italia](#) per segnalare la presenza di materiale pedopornografico online.

Gli alunni possono mostrare segni di tristezza o di ansia o di risentimento nei confronti di compagni o di altri e riferire spontaneamente o su richiesta l'accaduto ai docenti. I fatti riferiti possono essere accaduti anche al di fuori della scuola. Anche confrontandosi periodicamente con gli alunni sui rischi delle comunicazioni on-line, i minori possono riferire di fatti o eventi personali o altrui che

"allertano" l'insegnante.

Una "prova" di quanto riferito può essere presente nella memoria degli strumenti tecnologici utilizzati, può essere mostrata spontaneamente dall'alunno, può essere presentata da un reclamo dei genitori, può essere notata dall'insegnante che si accorge dell'infrazione in corso. I contenuti "pericolosi" comunicati/ricevuti a/da altri, messi scaricati in rete, ovvero le tracce che possono comprovare l'utilizzo incauto, scorretto o criminoso degli strumenti digitali utilizzabili anche a scuola attualmente dai minori (l'eventuale telefonino/smartphone personale e il pc collegato a internet) per gli alunni possono essere i seguenti:

- Contenuti afferenti alla privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);

- Contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);

- Contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc. -

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).

Per il telefono cellulare ci si può assicurare che l'alunno vittima salvi nel suo telefono ogni messaggio, voce/testo/immagine, conservando così il numero del mittente.

Gli insegnanti, anche con l'ausilio tecnico dell'Animatore digitale, possono provvedere ugualmente a conservare le prove della condotta incauta, scorretta o dell'abuso rilevate sui pc della scuola: soprattutto la data e l'ora, il contenuto dei messaggi e, se possibile, l'ID del mittente (es. username, mail, numero di telefono cellulare) o l'indirizzo web del profilo ed il suo contenuto. Qualora ci si dovesse accorgere che l'alunno, usando il computer, si sta servendo di un servizio di messaggistica istantanea, programma che permette di chattare in linea tramite testo, l'insegnante può copiare, incollare e stampare la conversazione. Per gli eventuali collegamenti non autorizzati a siti social network, video-hosting sites e altri website, l'insegnante può conservare il link, stampare la pagina o salvare la schermata su documento word. Per le e-mail si può stampare la mail o conservare l'intero messaggio, compresa l'intestazione del mittente. Conservare la prova è utile per far conoscere l'accaduto in base alla gravità ai genitori degli alunni, al Dirigente scolastico e per le condotte criminose alla polizia. Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno, quantunque riferite a fatti accaduti al di fuori del contesto scolastico, le notizie raccolte sono comunque comunicate ai genitori e per fatti rilevanti anche al Dirigente scolastico; per quelle criminose, anche alla polizia. In particolare la segnalazione viene fatta a entrambe le famiglie, se oltre alla vittima anche l'autore della condotta negativa è un altro alunno.

Per le segnalazioni di fatti rilevati sono previsti i seguenti strumenti che i docenti possono utilizzare sulla base della gravità dell'accaduto:

-Annotazione del comportamento sul registro e comunicazione scritta ai genitori, che la devono

restituire vistata;

-Convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti; x Relazione scritta al Dirigente scolastico. In base all'urgenza le comunicazioni formali possono essere precedute da quelle informali, effettuate per le vie brevi. Inoltre per i reati meno gravi la legge rimette ai genitori degli alunni la scelta di richiedere la punizione del colpevole, attraverso la querela.

Per i reati più gravi (es. pedopornografia) gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti). In particolare per i fatti criminosi, ai fini della denuncia, la relazione deve essere circostanziata, cioè redatta nel modo più accurato possibile, indicando i seguenti elementi: il fatto, il giorno dell'acquisizione del fatto nonché le fonti di prova già note e per quanto possibile, le generalità, il domicilio e quant'altro di utile a identificare la persona alla quale il reato è attribuito, la persona offesa, e tutti coloro che sono in grado di riferire circostanze rilevanti per la ricostruzione del fatto.

5.3. - *Gli attori sul territorio*

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

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

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

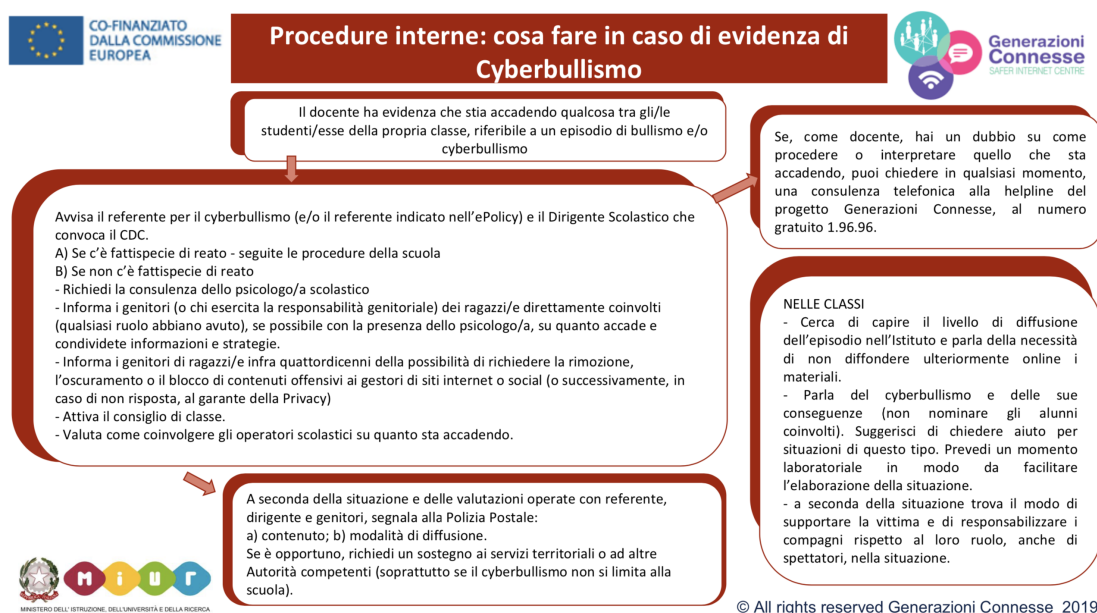
- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

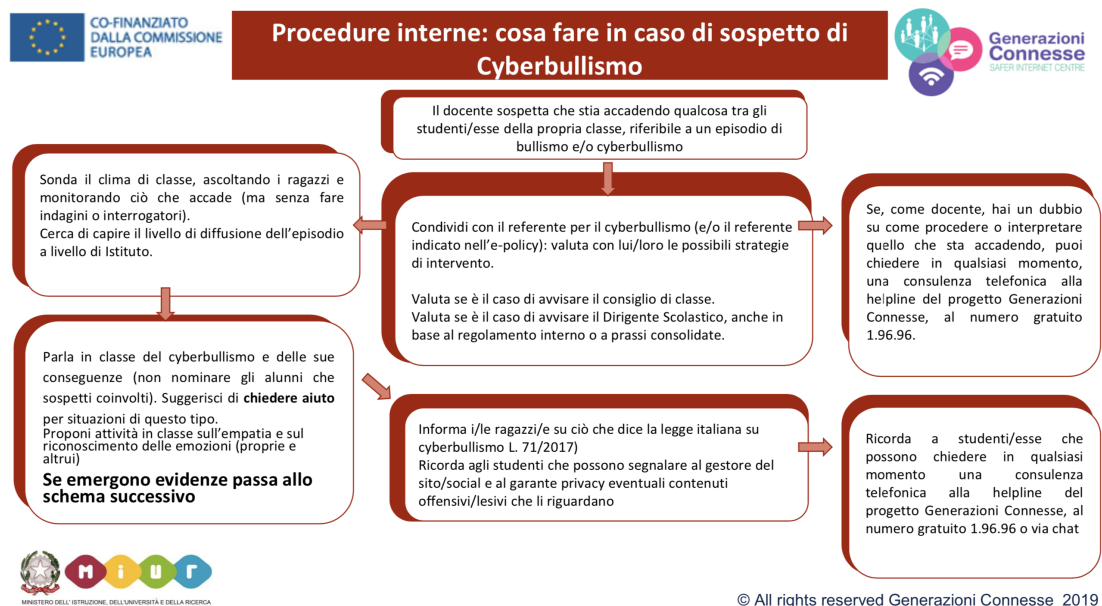
psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.

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

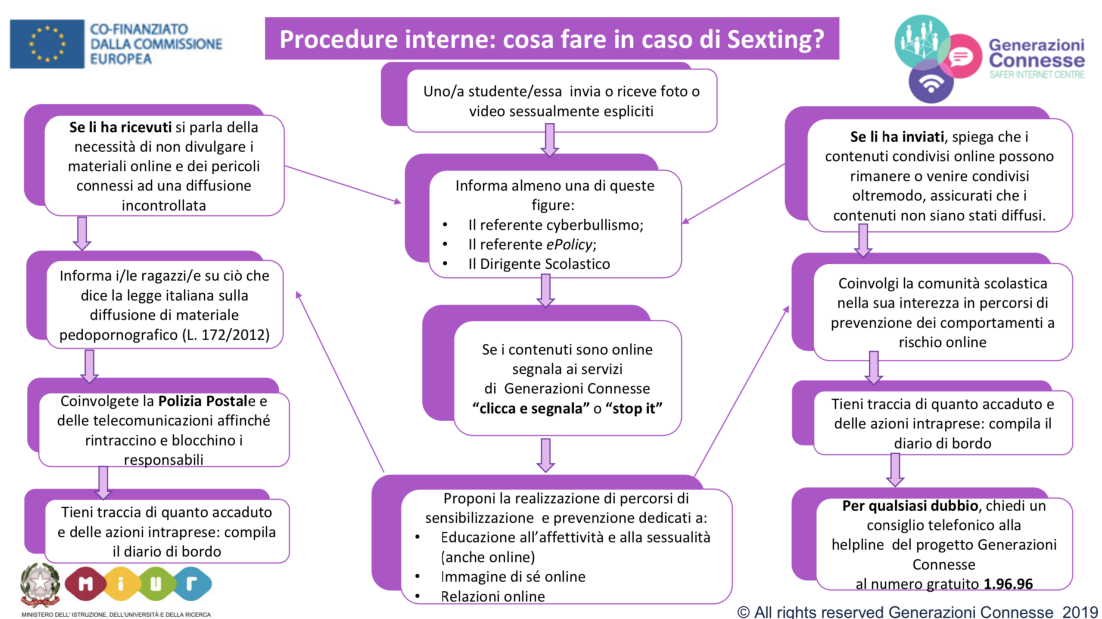
5.4. - Allegati con le procedure

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

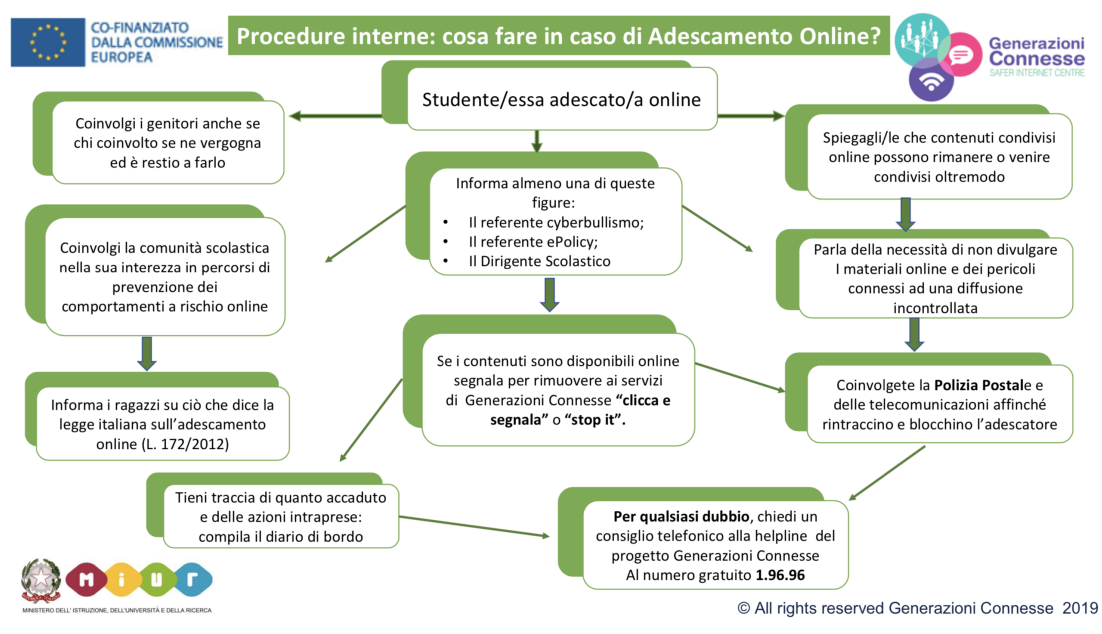




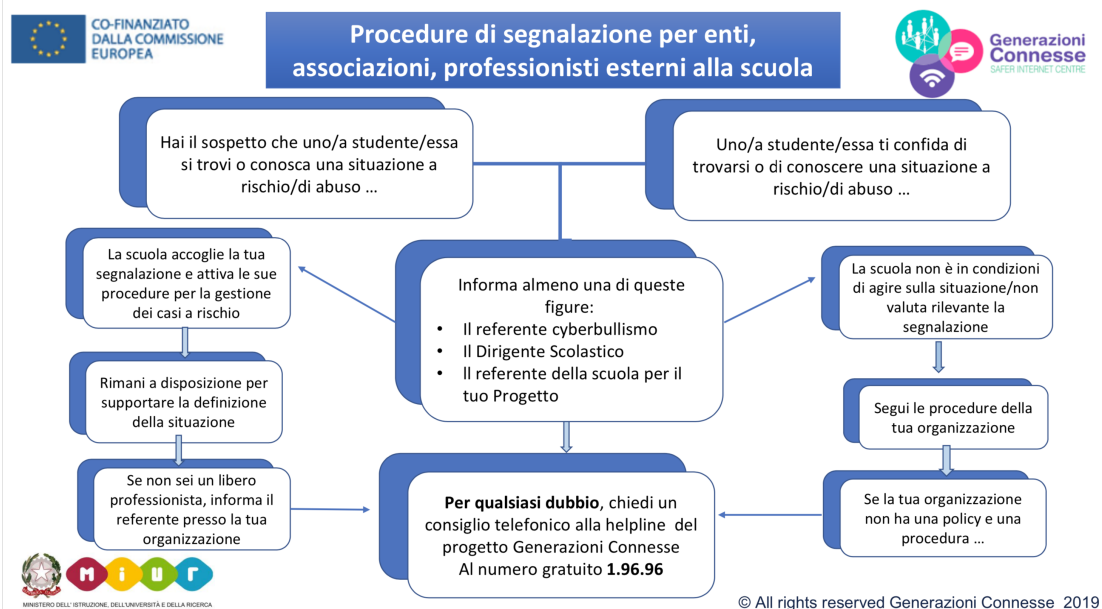
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

- [Scheda di segnalazione](#)

- [Diario di bordo](#)
- [iGloss@ 1.0 l'ABC dei comportamenti devianti online](#)
- [Elenco reati procedibili d'ufficio](#)

Il nostro piano d'azioni

Non è prevista nessuna azione.

