



SMS - "A. INVEGES"-SCIACCA
Prot. 0008078 del 16/12/2021
08 (Uscita)



Documento di ePolicy

AGMM054009

SMS - A. INVEGES

VIA A.DE GASPERI N.8/A - 92019 - SCIACCA - AGRIGENTO (AG)

Maria Angela Croce

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.

Come già detto prima, l'ePolicy è un documento programmatico autoprodotta dalla scuola volto a descrivere:

- il proprio approccio alle tematiche legate alle competenze digitali, alla sicurezza online e ad un uso positivo delle tecnologie digitali nella didattica;
- le norme comportamentali e le procedure per l'utilizzo delle Tecnologie dell'informazione e della comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione;
- le misure per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

Nello specifico la scuola media A. Inveges, che ha aderito al progetto "Generazioneio connesse" nell'anno scolastico 2021-2022, intende, mediante il documento, promuovere le seguenti iniziative:

- formare il personale interno circa le tematiche previste dalla policy;
- rendere consapevoli gli adolescenti dei rischi a cui si espongono quando navigano in rete;
- sensibilizzare i genitori sul tema della sicurezza online;
- costruire partenariati con enti e associazioni esterne.

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.

Bisogna, quindi, specificare, per 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, quali ruoli e responsabilità ricoprono.

Il Dirigente Scolastico

Il Dirigente Scolastico garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica. E' formato adeguatamente sulla sicurezza e sulla prevenzione di problematiche offline e online, in linea con il quadro normativo di riferimento e le indicazioni del MIUR; inoltre, promuove la cultura della sicurezza online e, ove possibile, dà il proprio contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC. Infine, ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

L'Animatore digitale

L'Animatore digitale supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, è uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica); inoltre, monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola, e ha il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

Il Referente bullismo e cyberbullismo

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

I Docenti

I Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle

TIC e della Rete. Integano parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica. I docenti accompagnano e supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete; hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

Il personale Amministrativo, Tecnico e Ausiliario (ATA)

Il personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il dirigente scolastico e con il personale docente tutto. Diverse figure che, in sinergia, si occupano ciascuno per la propria funzione, del funzionamento dell'Istituto scolastico che passa anche attraverso lo sviluppo della cultura digitale e dell'organizzazione del tempo scuola. Esiste, cioè, un concreto coinvolgimento del personale ATA nell'applicazione della [legge 107/15](#) (["La Buona Scuola"](#)) che concerne non solo il tempo scuola e il potenziamento dell'offerta formativa, ma anche le attività di formazione e autoformazione in tema di bullismo e cyberbullismo. Il personale ATA è coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo.

Gli Studenti e le Studentesse

Gli Studenti e le Studentesse dovrebbero, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola dovrebbero imparare a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le; dovrebbero partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education.

I Genitori

I Genitori, in continuità con l'Istituto scolastico, dovrebbero essere partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali; dovrebbero relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet. È estremamente importante che

accettino e condividano quanto scritto nell'ePolicy dell'Istituto.

Gli Enti educativi esterni e le associazioni

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola dovrebbero conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC; dovrebbero, inoltre, promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

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).

L'Istituto si doterà di un'informativa sintetica sull'ePolicy comprensiva delle procedure di segnalazione da condividere con tutte le figure che operano con studenti e studentesse e ciò per tutelare non solo questi ultimi e la scuola stessa, ma anche per porre in essere nuove modalità per rilevare, limitare e contrastare possibili pericoli legati a condotte educative non professionali.

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.

È necessario che il documento di ePolicy venga condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. Nello specifico è importante tener presente che:

- **condividere e comunicare il documento agli studenti e alle studentesse** significa dare loro una base di partenza per un uso consapevole e maturo dei dispositivi e della tecnologia informatica; dare loro regole condivise di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici; dare loro elementi per poter riconoscere e quindi prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e.
- **è importante condividere e comunicare il documento al personale scolastico** in modo da poter orientare tutte le figure sui temi in oggetto, a partire da un uso corretto dei dispositivi e della Rete in linea anche con il codice di comportamento dei pubblici dipendenti;
- **è fondamentale condividere e comunicare il documento ai genitori** sul sito istituzionale della scuola, nonché tramite momenti di formazione specifici e durante gli incontri scuola-famiglia.

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.

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

- **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.**

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.

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/la studente/ssa attraverso i servizi predisposti, qualora ciò fosse necessario.

E' necessario, inoltre, considerare il comportamento del personale scolastico riguardante le possibili infrazioni nelle quali il personale docente e non può incorrere se utilizza impropriamente i device o la Rete, nonché in quelle violazioni qualora non intervenga nella segnalazione di condotte improprie degli studenti/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.

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 d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti

Azioni da svolgere nei prossimi 3 anni:

- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori
- 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

Capitolo 2 - Formazione e curriculum

2.1. Curriculum 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.

In quest’ambito si seguono le indicazioni contenute nel PNSD (azione 14), in cui si individuano alcuni framework di riferimento per la definizione e lo sviluppo delle competenze digitali, tra cui il framework DIGCOMP, che prevede 21 competenze, di cui alcune specifiche nell’area della sicurezza.

1. **INFORMAZIONE:** identificare, localizzare, recuperare, conservare, organizzare e analizzare le informazioni digitali, giudicare la loro importanza e lo scopo.
2. **COMUNICAZIONE:** comunicare in ambienti digitali, condividere risorse attraverso strumenti on- line, collegarsi con gli altri e collaborare attraverso strumenti digitali, interagire e partecipare alle comunità e alle reti.

3. **CREAZIONE DI CONTENUTI:** creare e modificare nuovi contenuti (da elaborazione testi a immagini e video); integrare e rielaborare le conoscenze e i contenuti; produrre espressioni creative, contenuti media e programmare; conoscere e applicare i diritti di proprietà intellettuale e le licenze.

4. **SICUREZZA:** protezione personale, protezione dei dati, protezione dell'identità digitale, misure di sicurezza, uso sicuro e sostenibile.
 - Proteggere i dispositivi Proteggere i propri strumenti ed essere consapevole dei rischi in rete e delle minacce; conoscere le misure di protezione e sicurezza.

 - Proteggere i dati personali Comprendere i termini di servizio comuni; proteggere in modo attivo i dati personali; rispettare la privacy di altri soggetti; proteggersi dalle frodi in rete, dalle minacce e dal cyberbullismo.

 - Tutelare la salute Evitare i rischi per la salute connessi all'uso della tecnologia relativamente a minacce al benessere fisico e psicologico.

5. **PROBLEM-SOLVING:** identificare i bisogni e le risorse digitali, prendere decisioni informate sui più appropriati strumenti digitali secondo lo scopo o necessità, risolvere problemi concettuali attraverso i mezzi digitali, utilizzare creativamente le tecnologie, risolvere problemi tecnici, aggiornare la propria competenza e quella altrui.

Pertanto, questa scuola si propone un programma di progressiva educazione alla sicurezza, online come parte del curriculum scolastico. Si impegna a sviluppare una serie di competenze e comportamenti adeguati alle età degli alunni e ad esperienza, tra cui:

- programmare attività e far partecipare gli alunni a laboratori di utilizzo consapevole e appropriato delle TIC;
- capire il comportamento accettabile quando si utilizza un ambiente online, vale a dire, essere educato, non utilizzare comportamenti inappropriati, mantenere

le informazioni personali private;

- conoscere le conseguenze disciplinari della scuola, civili e penali in caso di denuncia e riscontro oggettivo di infrazioni inerente un utilizzo scorretto degli smartphone e contrario alla presente policy o al regolamento di istituto;
- capire il motivo per cui non devono pubblicare foto o video di altri senza il loro permesso capire il motivo per cui qualsiasi materiale scritto, pubblicato e postato sui social è sempre tracciabile e può rimanere per sempre
- capire che condividere è essere ugualmente responsabili di ciò che vi è all'interno del gruppo capire perché 'amici' on-line potrebbero non essere chi dicono di essere e di comprendere perché dovrebbero fare attenzione in un ambiente online;
- capire il motivo per cui non dovrebbero inviare o condividere resoconti dettagliati delle loro vite personali e informazioni di contatto;
- comprendere l'impatto di bullismo online, sexting, grooming e sapere come cercare aiuto se sono in pericolo;
- sapere come segnalare eventuali abusi tra cui il bullismo on-line e come chiedere aiuto ai docenti, ai genitori, se si verificano problemi quando si utilizzano le tecnologie Internet; utilizzare con attenzione Internet per garantire che si adatti alla loro età e supporti gli obiettivi di apprendimento per le aree curriculari specifiche.
- sviluppare una serie di strategie per valutare e verificare le informazioni prima di accettarne l'esattezza

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.

Il corpo docente parteciperà a corsi di formazione anche nell'ambito di piani nazionali, oltre che ad iniziative organizzate dall'istituzione o dalle scuole associate in rete. Il percorso complesso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica dovrà avere carattere permanente e, pertanto, dovrà prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva anche all'interno dell'istituto, con la condivisione delle conoscenze dei singoli, la partecipazione alle iniziative promosse dall'Amministrazione centrale e dalle scuole polo; può comprendere, altresì, la fruizione dei materiali messi a disposizione sulla sezione del sito dedicata al PNSD con bacheche virtuali appositamente create e corsi di aggiornamento online.

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

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

amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

L'Istituto ha aderito alle attività formative, promosse dal MIUR nell'ambito del PNSD, organizzate dagli snodi formativi. Si prevede l'attivazione di iniziative di formazione facendo ricorso a soggetti esterni e/o al personale docente interno alla scuola che abbia acquisito competenze sull'innovazione didattica. Il percorso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica deve diventare un processo permanente che deve prevedere anche momenti di autoaggiornamento, di formazione personale o collettiva.

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.

Il "Patto di Corresponsabilità" è un documento centrale per ogni istituzione scolastica e per la comunità educante tutta. Per questo, recentemente è stato avviato dal Miur un percorso di revisione finalizzato a definire in modo più dettagliato modalità, tempi e ambiti della partecipazione da parte di genitori e studenti alla vita scolastica. E ciò, anche al fine di creare una maggiore collaborazione e condivisione degli interventi di formazione e di contrasto al bullismo e al cyberbullismo all'interno della comunità educante.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

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

Scegliere almeno 1 di queste azioni

- 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.

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'accesso ai dati riportati nel registro elettronico (ritardi, assenze, note e valutazioni) è riservato ai genitori tramite la consegna di una password di accesso strettamente personale.

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’istituto si è dotato di un regolamento sull’uso dei laboratori che prevede una parte dedicata all’utilizzo di internet.

La gestione degli account degli utenti avviene in modo differenziato per docenti, studenti e personale amministrativo.

Sui computer è possibile effettuare installazioni e aggiornamenti di software solo tramite la password di amministratore, fornita al personale di assistenza tecnica, alla Funzione Strumentale per l’innovazione tecnologica e all’Animatore Digitale.

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.

Il registro elettronico rappresenta lo strumento privilegiato per le comunicazioni e la condivisione di documenti tra il personale della scuola.

Gli insegnanti accedono al registro elettronico attraverso una password personale che non può essere comunicata a terzi, né agli alunni.

Il sito dell’Istituto prevede un’area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali, avvisi di carattere generale.

Sul sito della scuola i contenuti di carattere amministrativo sono pubblicati dalla segreteria e dalla dirigenza.

Gli insegnanti sono tenuti a controllare la strumentazione in aula e i dispositivi personali degli studenti, poiché il loro uso è permesso solo su autorizzazione del

docente.

Abitualmente nella didattica non vengono utilizzati i social network, neanche da parte dell'istituzione scolastica e il personale scolastico non è autorizzato a servirsene per nome e per conto della stessa. Si potrà fare eccezione in caso di partecipazione ad iniziative specifiche, previa richiesta di autorizzazione e supervisione del Dirigente.

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.

Ogni docente può utilizzare la connessione, tramite il pc fornito dalla scuola o il pc personale, per la gestione del registro elettronico e per l'attività didattica; i docenti non possono utilizzare la rete della scuola per scopi privati.

I dispositivi personali possono essere utilizzati dagli studenti solo per le attività didattiche, solo su autorizzazione e supervisione del docente.

Nel regolamento dell'Istituto sono inserite le sanzioni disciplinari in caso di uso scorretto dei cellulari da parte degli studenti. Il dirigente, i docenti e il personale ATA hanno il dovere di vigilare sui comportamenti dei ragazzi e delle ragazze e di segnalare eventuali infrazioni suscettibili di sanzioni disciplinari.

I docenti non devono utilizzare telefoni cellulari durante le attività didattiche (C.M. 25 agosto 1998, n. 362), sia per consentire un sereno ed efficace svolgimento delle attività, sia per offrire agli alunni un modello educativo di riferimento esemplare. L'uso ne è permesso soltanto per agevolare i compiti previsti istituzionalmente e dal Regolamento d'Istituto.

L'alunno potrà utilizzare apparecchiature elettroniche solo rispettando quanto segue:

- il personal computer, il tablet e l'iPad sono strumentazioni elettroniche il cui uso è consentito in classe esclusivamente per attività didattiche e, pertanto, il loro utilizzo deve essere coerente con le richieste fatte dai docenti e, in genere, dalla scuola;
- ogni alunno è personalmente responsabile del materiale prodotto o visionato, dei danni eventualmente causati a terzi e delle violazioni di legge effettuate con l'utilizzo di tali strumentazioni; i docenti hanno la facoltà, in qualunque momento, di prendere visione dei dati trattati in classe. Sono vietati i collegamenti a Internet da proprio apparecchio.
- all'interno della scuola, la lan e internet sono aree di comunicazione e condivisione di informazioni strettamente didattiche e non possono essere utilizzate per scopi diversi; qualunque uso della connessione che violi le leggi civili e penali in merito e il Regolamento d'Istituto è vietato;
- ogni tentativo di forzare o manomettere la rete dell'istituto e le sue protezioni sarà sanzionato come grave infrazione disciplinare;
- è vietato l'uso dell'applicazione della fotocamera e dei registratori audio/video se non autorizzato dall'insegnante, in quanto l'uso non autorizzato e scorretto rappresenta grave violazione della privacy.
- tutti gli alunni sono tenuti a rispettare le regole di correttezza e riservatezza in campo telematico, nonché eventuali implicazioni riguardanti la proprietà intellettuale del materiale utilizzato;
- gli alunni sono tenuti a mettere in carica le proprie apparecchiature elettroniche a casa, in modo da poterle utilizzare a scuola senza cavi di alimentazione. L'utilizzo scorretto delle apparecchiature elettroniche a scuola comporterà l'adozione di provvedimenti disciplinari da parte dell'organo di competenza. In presenza di situazioni e/o episodi gravi, il Dirigente Scolastico provvederà alle opportune segnalazioni alle autorità competenti.

Ogni studente è responsabile dell'integrità degli arredi e del materiale didattico che la

scuola gli affida: coloro che provocheranno guasti al materiale o danni alle suppellettili della scuola o del Comune saranno tenuti a risarcire i danni.

Il nostro piano d'azioni

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

- 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

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

- 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 il personale adulto 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.

La diffusione delle tecnologie digitali e dell'accesso alla Rete già nei primissimi anni di vita sta portando profondi cambiamenti nelle dinamiche relazionali e in quelle identitarie, trasformando linguaggi, modalità di comunicazione, abitudini e stili di vita e offrendo inedite potenzialità di crescita.

Se, dunque, le Tecnologie dell'Informazione e della Comunicazione (TIC) sono parte integrante della vita quotidiana dei più giovani, in quanto strumenti privilegiati di comunicazione e di relazione, ma anche di informazione, studio, creatività e partecipazione, esse pongono però delle questioni associate alla "sicurezza" e al comportamento sociale. Non bisogna, infatti, cadere nello stereotipo di una categoria uniforme di bambini/e e adolescenti "competenti", sollevando gli adulti dal proprio ruolo educativo e dalla responsabilità di promuovere presso i più giovani un uso consapevole e quindi anche un uso integrativo (e non sostitutivo) delle tecnologie digitali. Siamo di fronte ad una realtà complessa, pensata prevalentemente per un mondo adulto e nella quale trovano spazio contenuti e comportamenti potenzialmente dannosi.

I rischi online rappresentano tutte quelle situazioni problematiche derivanti da un uso non consapevole e non responsabile delle tecnologie digitali da parte di bambini/e, ragazzi e ragazze: adescamento online, cyberbullismo, sexting, violazione della privacy, pornografia (recenti ricerche hanno sottolineato come la maggior parte degli adolescenti reperisca in Rete informazioni inerenti la sessualità, col rischio, spesso effettivo, del diffondersi di informazioni scorrette e/o l'avvalorarsi di falsi miti), pedopornografia (con questo termine si intende qualsiasi foto o video di natura sessuale che ritrae persone minorenni), gioco d'azzardo o gambling, internet addiction, videogiochi online (alcuni rischi associati possono essere ad esempio: contatti impropri con adulti, contenuti violenti e/o inadeguati; acquisti incontrollati, etc.), esposizione a contenuti dannosi o inadeguati (es. contenuti razzisti, che inneggiano al suicidio, che promuovono comportamenti alimentari scorretti, etc.), etc.

Partendo da questo punto di vista, vanno promosse nei più giovani le necessarie competenze e capacità, al fine di una protezione adeguata, ma anche al fine di un utilizzo consapevole che sappia sfruttare le potenzialità delle tecnologie digitali e gestirne le implicazioni.

Due sono i principali strumenti in questo caso da mettere in campo e si sintetizzano in interventi di Sensibilizzazione e Prevenzione.

Interventi di sensibilizzazione

Si parla spesso di interventi o campagne di sensibilizzazione, si tratta in questi casi di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento.

Molte campagne di sensibilizzazione hanno, ad esempio, una risonanza internazionale che può mirare a:

- mettere in luce una determinata problematica o condizione,
- chiedere ad una determinata utenza di attivarsi per una causa,
- raccogliere dei fondi.

Altri interventi possono, invece, essere mirati a piccoli gruppi o comunità (come ad esempio la comunità scolastica), con l'obiettivo di coinvolgere un gruppo ristretto di persone affinché agiscano insieme in favore di una causa in cui credono.

Quali possono essere i benefici di un'attività di sensibilizzazione?

- accrescere la consapevolezza nel gruppo target di riferimento circa un determinato tema/bisogno/problema che potrebbe presentarsi in quel gruppo;
- incoraggiare il gruppo a modificare i propri comportamenti rendendoli più funzionali;
- diffondere all'esterno del gruppo di riferimento e quindi tra l'opinione pubblica una certa consapevolezza rispetto all'argomento di interesse;
- facilitare il coinvolgimento di soggetti esterni in modo da mettere insieme diverse idee per lavorare ad un obiettivo comune.
- favorire la diffusione di informazioni e servizi disponibili all'utilità collettiva (ad esempio, si può pensare ad un intervento di sensibilizzazione per promuovere la conoscenza dell'ePolicy nella comunità scolastica).

La sensibilizzazione può costituire il primo passo verso un cambiamento positivo, ma per far sì che l'intervento sia efficace, è importante che sia chiara l'azione verso cui i soggetti devono impegnarsi. **Due sono gli aspetti che bisogna tenere in considerazione:**

- la consapevolezza dello status quo;
- la motivazione al cambiamento.

Per far sì che un intervento di sensibilizzazione sia efficace, è quindi importante fornire ai beneficiari informazioni chiare su quello che è lo stato attuale del tema che vogliamo trattare (ad es. se si vuol trattare il tema del Cyberbullismo, sarà opportuno fornire informazioni su quali sono le caratteristiche del fenomeno e i dati rappresentativi). In questo modo gli utenti avranno tutte le informazioni necessarie per avere una fotografia chiara del contenuto che stiamo trattando e del perché è necessario impegnarsi verso un cambiamento (motivazione al cambiamento).

In sintesi, è opportuno tenere in considerazione i seguenti aspetti:

- spingere le persone a desiderare un cambiamento;
- porre in evidenza la possibilità di generare un cambiamento;
- individuare le azioni che consentono di produrre il cambiamento.

Un'attività di sensibilizzazione dovrebbe quindi fornire non solo le informazioni necessarie, ma anche illustrare le possibili soluzioni o comportamenti da adottare.

Interventi di prevenzione

Il concetto di **prevenzione** nasce in ambito epidemiologico e seguendo quanto

riportato dal Ministero della Salute si può sintetizzare come un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere e conservare lo stato di salute ed evitare l'insorgenza di malattie.

Parlando di prevenzione in ambito digitale si potrebbe tradurre quanto appena detto con 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.

Se il problema della "sicurezza" è difficilmente riconducibile esclusivamente all'esistenza in sé di alcuni rischi, più o meno gravi e insidiosi, appare chiaro dunque come le migliori strategie di intervento siano di carattere prevalentemente preventivo.

La letteratura storicamente distingue tre livelli di prevenzione: primaria, secondaria e terziaria (Caplan, G. (1964). Principles of preventive psychiatry. New York: Basic Books), nel dibattito comune questa classificazione è presente ancora oggi, ma la comunità scientifica internazionale non è concorde e si preferisce utilizzare la classificazione proposta dall'Institute of Medicine che distingue i tre livelli in:

1. **Prevenzione Universale.** Un programma di questo tipo parte dal presupposto che tutti gli studenti siano potenzialmente a rischio. Si tratta quindi di interventi diretti al grande pubblico o a un intero gruppo di una popolazione che non è stato identificato sulla base del rischio individuale. Efficacia: trattandosi di programmi ad ampio raggio gli effetti di questi programmi possono essere modesti se confrontati con programmi che "trattano" un gruppo con un problema specifico. Tuttavia, questi interventi possono produrre cambiamenti in grandi popolazioni (ad es. si pensi ad un programma dedicato alle competenze emotive, oppure alla cittadinanza digitale).
2. **Prevenzione Selettiva.** Un programma dedicato ad un gruppo di studenti in cui il rischio online è presente. In questo caso la presenza del rischio è stata individuata tramite precedenti indagini, segnalazioni fatte dalla scuola, oppure dalla conoscenza della presenza di fattori di rischio in quel determinato territorio. In questi casi gli interventi sono mirati e prevedono programmi formativi strutturati che hanno l'obiettivo di migliorare le competenze digitali e le strategie di problem solving. Può essere un valido programma se si osservano casi in cui la prevenzione universale non ha dato gli esiti previsti.
3. **Prevenzione Indicata.** Un programma di intervento sul caso specifico, è quindi pensato e strutturato per adattarsi agli/lle studenti/studentesse con l'obiettivo di ridurre i comportamenti problematici, oppure dare supporto alle vittime. Per la sua natura questo tipo di intervento si avvale di professionalità diverse perché spesso affronta problemi legati alla salute mentale del minore per cui è opportuno coinvolgere anche la famiglia del/lla ragazzo/a.

Il modello diviso in tre livelli può essere un'utile guida per affrontare e prevenire ogni possibile situazione di disagio, è tuttavia comprensibile la difficoltà di poter strutturare soluzioni ed interventi multilivello da parte dell'Istituzione Scolastica senza

il supporto di altri attori. I programmi che possono essere realizzati con maggiore frequenza ricadono nel primo livello di Prevenzione Universale e sono sicuramente consigliati proprio perchè vanno a formare e consolidare quelle competenze educative di base necessarie a poter gestire le situazioni di vita che i/le ragazzi/e sperimentano online.

Come sappiamo, le dimensioni che il fenomeno coinvolge sono molteplici e non puramente tecniche e si rifanno alla capacità dei più giovani di gestire situazioni complesse che richiedono: la capacità di gestire la relazione con l'altro/a diverso/a da sé, le dimensioni dell'affettività e della sessualità, il riconoscimento di un limite, anche, ma non solo, legato ad una dimensione di legalità, l'utilizzo sicuro e consapevole delle tecnologie digitali.

Per questo motivo la scuola deve rafforzare la sua capacità di rispondere anche a questi bisogni attraverso strumenti e misure specifiche. Allo stesso modo quando un evento problematico connesso ai rischi online coinvolge il contesto scolastico, è fondamentale per la scuola poter dare una risposta il più possibile integrata, che trovi la sua espressione di indirizzo in procedure chiare di cui deve dotarsi e che includano la collaborazione (prevedendo accordi specifici) con la rete dei servizi locali (in primis le ASL e la Polizia Postale).

Inoltre, la responsabilità dell'azione preventiva ed educativa chiama in campo diverse agenzie educative oltre alla scuola, come la famiglia, ma non solo (istituzioni, associazioni, società civile, etc.), ciascuna con un proprio compito nei confronti di bambini e bambine e di adolescenti. Tali agenzie sono chiamate a collaborare ad un progetto comune, nell'ambito di funzioni educative condivise. La necessità di questa collaborazione nasce, più o meno consapevolmente, dal riconoscimento sia da parte dei genitori che da parte degli insegnanti della rispettiva difficoltà a svolgere da soli la propria funzione formativa ed educativa. E questo, anche a causa della sproporzione tra le competenze sempre crescenti che le tecnologie digitali richiedono loro e quelle che si avvertono di possedere. La necessità di supportare un uso positivo e consapevole delle TIC da parte dei più giovani, sia in un'ottica di tutela dai rischi potenziali che nella valorizzazione delle opportunità esistenti, pone la scuola e i genitori di fronte alla sfida di riconsiderare la propria identità, il proprio ruolo educativo e le proprie risorse, oltre allo stato dei rapporti reciproci per un patto educativo da rinnovare costantemente.

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).

La Scuola Secondaria di 1° grado "A. Inveges" in ottemperanza alla normativa ha nominato un referente e costituito un Team Anti bullismo e per l'emergenza denominato "BullOut! Diciamo no al bullismo", formato dai seguenti membri:

- Dirigente scolastico - prof.ssa Maria Angela Croce;
- Referente per il contrasto del bullismo e cyberbullismo - prof.ssa Maria Mattia Lovoy;
- Referente per la legalità -prof.ssa Maria Grazia Curreri;
- Animatore digitale- prof. Mario Testoni;

- Docente FS Area inclusione- prof. Domenico Lorenzo Navarra.

Ma quali sono le caratteristiche specifiche del cyberbullismo rispetto al bullismo cosiddetto tradizionale?

Il cyberbullismo è una forma di prepotenza virtuale messa in atto attraverso l'uso di Internet e delle tecnologie digitali. Spesso i termini bullismo e cyberbullismo vengono usati impropriamente e si riconducono ad essi i più svariati episodi di violenza o offese fra ragazzi/e. Bullismo e cyberbullismo hanno, però, connotati ben precisi e non vanno confusi con altre problematiche del mondo giovanile.

Il termine cyberbullismo viene coniato dall'educatore canadese Bill Belsey nel 2002, ma una prima vera definizione del fenomeno viene elaborata solo qualche anno dopo. Nel 2006 Smith e collaboratori definirono il cyberbullismo come:

“Un atto aggressivo e intenzionale perpetrato da un individuo o da un gruppo, attraverso l'uso delle nuove tecnologie della comunicazione, in modo ripetuto e continuato nel tempo, contro una vittima che non può facilmente difendersi” (in Smith P.K., Mahdavi J., Carvalho C., e Tippett N., An investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbullying. A Report to the Anti-Bullying Alliance, 2006, p.6).

Nel bullismo tradizionale, solitamente, la vittima che viene presa di mira è percepita come più debole e incapace di difendersi.

Il più forte, quindi, assume atteggiamenti prevaricatori nei confronti del più debole, a partire da una certa “asimmetria di potere”.

Ciò, naturalmente, può accadere anche nel caso del cyberbullismo. Mentre nel bullismo tradizionale, però, il potere presenta connotati ben precisi, potrebbe essere, ad esempio, di tipo fisico (legato alla forza o alla statura) o sociale (legato alla popolarità), il potere online può derivare semplicemente dal possesso di specifiche competenze o di alcuni contenuti (immagini, video, confessioni) che potrebbero essere utilizzati per danneggiare la vittima.

Solitamente, quando si parla di cyberbullismo o di bullismo è necessario che vittima e bullo/cyberbullo siano minori o comunque adolescenti (sono esclusi, quindi, dalla definizione episodi di prevaricazione che avvengono fra adulti o fra un adulto e un minore).

Un'altra definizione di cyberbullismo è quella che ci fornisce la Legge Ferrara, ovvero la l. 71/2017 [“Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo”](#) (che affronteremo in modo più approfondito più avanti). Il testo 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 online 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” (Art. 1- Comma 2).

Le caratteristiche del fenomeno

Ma quali sono le caratteristiche specifiche del cyberbullismo rispetto al bullismo cosiddetto tradizionale? Come sottolinea la Willard i tratti specifici del bullismo online sono correlati all’impatto che le tecnologie digitali hanno nella vita dei ragazzi (e di tutti noi) e alle caratteristiche stesse della Rete (Willard, N. (2005), *Educator’s guide to cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress*, Research Press, Illinois). Vediamole a seguire:

- L’impatto: la diffusione di materiale tramite Internet è incontrollabile e non è possibile prevederne i limiti (anche se la situazione migliora, video e immagini potrebbero restare online e continuare a diffondersi). Un contenuto offensivo e denigratorio online può, quindi, diventare virale e distruggere in alcuni casi la reputazione della vittima. Nelle situazioni più gravi, le vittime di cyberbullismo si trovano costrette a dover cambiare scuola o addirittura città, ma questo spesso non le aiuta. La Rete, si sa, è ovunque.
- La convinzione dell’anonimato: chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile. Sentendosi protetti dall’anonimato ci si sente liberi e più forti nel compiere atti denigratori, senza il timore di essere scoperti. È importante tenere bene a mente, però, che quello dell’anonimato è un “falso mito della Rete”. Ogni nostra azione online è, infatti, rintracciabile e riconducibile a noi con gli strumenti opportuni o con l’intervento della Polizia Postale. L’anonimato del cyberbullo, inoltre, è anche uno dei fattori che stanno alla base del forte stress percepito dalla vittima, la quale molte volte non può dare né un nome e né un volto al proprio aggressore;
- L’assenza di confini spaziali: il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l’individuo dei suoi spazi-rifugio. La vittima può essere raggiungibile anche a casa e vive nella costante percezione di non avere vie di fuga. Spegnerne il cellulare o il computer non basta, così come cancellare tutti i propri profili social. Il solo pensiero che eventuali contenuti denigratori continuino a diffondersi online è doloroso e si accompagna ad un senso costante di rabbia e impotenza.
- L’assenza di limiti temporali: può avvenire a ogni ora del giorno e della notte.
- L’indebolimento dell’empatia: esistono cellule chiamate neuroni specchio che ci permettono di “leggere” gli altri quando li abbiamo di fronte, capirli e di provare emozioni simile a quelle che loro provano, proprio come se fossimo di fronte ad uno specchio. Tale sensazione è data dall’attivazione di una

particolare area del cervello. Quando le interazioni avvengono prevalentemente online la funzione speciale di questi neuroni viene meno (mancando la presenza fondamentale dell'altro che è sostituito dal dispositivo). La riduzione di empatia che ne consegue può degenerare nei comportamenti noti messi in atto dai cyberbulli.

- Il feedback non tangibile: il cyberbullo non vede in modo diretto le reazioni della vittima e, ancora una volta, ciò riduce fortemente l'empatia e il riconoscimento del danno provocato.

Per questo non è mai totalmente consapevole delle conseguenze delle proprie azioni. L'impossibilità di vedere con i propri occhi l'eventuale sofferenza e umiliazione provata dalla vittima fa sì che il tutto venga percepito come "uno scherzo" divertente a cui partecipare, di cui ridere o a cui essere indifferenti. Inoltre, il cyberbullismo non lascia segni fisici evidenti sulla vittima e si consuma in un contesto virtuale che spesso viene percepito dai ragazzi come non "reale", come un mondo ludico a sé stante.

Per questo il fenomeno viene talvolta sottovalutato anche dal mondo adulto, familiare e scolastico.

La mediazione tecnologica, infatti, porta ad un certo distanziamento fra aggressore e vittima, causando quello che Bandura ha definito come "disimpegno morale". Si tratta di un indebolimento del controllo morale interno dell'individuo, con la conseguente minimizzazione delle responsabilità individuali. Tale fenomeno vale non solo per il cyberbullo, ma anche per i cosiddetti bystander, ossia coloro che sono spettatori dei fatti.

A ciò si aggiungono altre convinzioni o tendenze frequenti nell'uso della Rete sia da parte dei giovani che degli adulti:

- Percezione che online non ci siano norme sociali da rispettare: fra i giovani spesso vige la falsa convinzione secondo cui la Rete sia uno spazio virtuale lontano dalla realtà, in cui vige libertà assoluta e in cui regole e norme sociali della vita quotidiana non valgono;
- La sperimentazione online di identità e personalità multiple: la Rete è per i minori il luogo virtuale per eccellenza in cui mettersi in gioco "fingendo di essere ciò che non si è" per il semplice gusto di sperimentare nuove forme di identità e comportamento;
- Il contesto virtuale come un luogo di simulazione e giochi di ruolo: "la vita sullo schermo" e tutti i comportamenti messi in atto online vengono percepiti solo come un gioco.
- Diffusione di responsabilità: tutti quelli che partecipano anche solo con un like o un commento diventano, di fatto, corresponsabili delle azioni del cyberbullo facendo accrescere la portata dell'azione; mettere un "like" su un social network commentare o condividere una foto o un video che prende di mira qualcuno o semplicemente tacere pur sapendo, mette ragazzi e ragazze nella condizione di avere una responsabilità.

Ma d'altro canto sono proprio loro che possono "fare la differenza" perché la responsabilità è condivisa: il gruppo "silente" che partecipa senza assumersi la responsabilità, rappresenta, in realtà, anche l'elemento che può fermare una situazione di cyberbullismo. E questo appunto costituisce un gancio educativo.

È possibile suddividere gli atti di cyberbullismo in due grandi gruppi:

1. cyberbullismo diretto: il bullo utilizza strumenti di messaggistica istantanea (es. sms, mms) che hanno un effetto immediato sulla vittima, poiché diretti esclusivamente a lei.
2. cyberbullismo indiretto: il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima anche da un punto di vista psicologico.

È molto importante sottolineare come il cyberbullismo non sia una problematica che riguarda unicamente vittima e cyberbullo. È un fenomeno sociale e di gruppo. Infatti, centrale è il ruolo delle agenzie educative e di socializzazione (formali e informali) più importanti per gli adolescenti: la famiglia, la scuola, i media, le tecnologie digitali e il gruppo dei pari.

Il nostro Istituto intende prevenire e affrontare la tematica del cyberbullismo mediante diverse azioni:

- una progettazione curriculare che prevede interventi di sensibilizzazione e informazione rivolti agli alunni dei tre ordini di classe da parte dei docenti delle aree Linguistica/Espressiva, Artistica/Musicale, Benessere/Sport/Prevenzione/Sicurezza.
- la creazione di una cassetta riservata in cui gli alunni potranno lasciare segnalazioni su eventuali episodi di bullismo ricevuti o visti;
- la promozione della Giornata nazionale contro il bullismo;
- la partecipazione ad eventi/concorsi locali e nazionali;
- il coinvolgimento di Enti esterni, Forze dell'Ordine, (Polizia di Stato, Polizia Postale, Guardia di Finanza), Magistrati, Psicologi, in attività formative rivolte agli alunni e all'intera comunità;
- la creazione sul sito istituzionale di un'apposita sezione che rimanda al sito del Min. Istr. www.generazioniconnesse.it per informazioni di carattere generale.

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 crede fermamente nel valore educativo e formativo della **Memoria**, che diventa monito e argine rispetto alla deriva verso cui conduce l’odio per il diverso. Per cui si celebreranno in vario modo le diverse Giornate della Memoria, del Ricordo, della lotta contro ogni forma di discriminazione.

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?

Secondo uno studio del [King's College di Londra](#) più del 23% dei giovani intervistati ha una relazione disfunzionale con il proprio smartphone. Stati d’ansia provocati dalla

ricerca e dall'uso compulsivo del cellulare che, nei casi più gravi, si associano a veri e propri stati depressivi. In Italia, secondo una [ricerca](#), ben il 45% degli studenti (6.671 giovani tra gli 11 e i 25 anni) dichiara di passare sul web almeno 5-6 ogni giorno e il tempo trascorso online raggiunge picchi più alti nel fine settimana: 1 intervistato su 5 dice di sentirsi a disagio o comunque va in ansia quando manca la connessione alla Rete e cresce in contemporanea la percentuale di coloro che manifestano attacchi di panico quando finiscono i giga e le promozioni tariffarie a cui sono abbonati (circa 1 su 3). Ancora, secondo l'Istat, ["nel 2018, l'85,8% dei ragazzi tra 11 e 17 anni di età utilizza quotidianamente il telefono cellulare. Il 72% dei ragazzi in quella stessa fascia di età naviga in Internet tutti i giorni. Questa quota è cresciuta molto rapidamente passando dal 56,2 al 72,0% nell'arco di un quadriennio. Le più frequenti utilizzatrici del cellulare e della rete sono le ragazze, l'87,5% delle quali usa il cellulare quotidianamente e il 73,2% accede a Internet tutti i giorni \(quota che sale all'84,9% se ci si concentra sulle adolescenti tra i 14 e i 17 anni\). L'accesso ad Internet è fortemente trainato dalla diffusione degli smartphone. Soltanto il 27,7% dei ragazzi, infatti, usa il pc tutti i giorni e questa quota è in forte calo rispetto al 40,5 del 2014"](#).

La dipendenza da Internet, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica che deve attenzionare il fenomeno e fornire gli strumenti agli studenti e alle studentesse affinché questi siano consapevoli dei rischi che comporta l'iperconnessione.

La S.I.I.Pa.C., la [Società Italiana Intervento Patologie Compulsive](#), definisce la dipendenza da Internet come progressivo e totale assorbimento del soggetto alla Rete; di seguito alcune caratteristiche specifiche:

- Dominanza. L'attività domina i pensieri ed il comportamento del soggetto, assumendo un valore primario tra tutti gli interessi.
- Alterazioni del tono dell'umore. L'inizio dell'attività provoca cambiamenti nel tono dell'umore. Il soggetto prova un aumento d'eccitazione o maggiore rilassatezza come diretta conseguenza dell'incontro con l'oggetto della dipendenza.
- Conflitto. Conflitti inter-personali tra il soggetto e coloro che gli sono vicini, conflitti intra-personali interni a se stesso, a causa del comportamento dipendente.
- Ricaduta. Tendenza a ricominciare l'attività dopo averla interrotta.

I segnali patologici di questo che viene descritto come "un vero e proprio abuso della tecnologia", anche denominato "Internet Addiction Disorder" (I.A.D. coniato dallo psichiatra Ivan Goldberg 1996), sono specifici così come accade per le altre dipendenze più "tradizionali". In particolare, si hanno: la tolleranza ossia quando vi è un crescente bisogno di aumentare il tempo su internet e l'astinenza quando, cioè, vi è l'interruzione o la riduzione dell'uso della Rete che comporta ansia, agitazione psicomotoria, fantasie, pensieri ossessivi (malessere psichico e/o fisico che si manifesta quando s'interrompe o si riduce il comportamento). Tutto questo ha ripercussioni sulla sfera delle relazioni interpersonali che diventano via via più povere

e alle quali si preferisce il mondo virtuale, con alterazioni dell'umore e della percezione del tempo.

Da sottolineare, la nomofobia (nomo deriva da "no-mobile") termine usato per categorizzare quei soggetti che sperimentano emozioni negative, quali ansia, tristezza e rabbia quando non sono connessi con il proprio smartphone. Anche qui i dati dell'Osservatorio nazionale adolescenza sembrano parlare chiaramente: ["quasi 8 adolescenti su 10 hanno paura che si scarichi il cellulare o che non gli prenda quando sono fuori casa \(un dato in forte crescita se si pensa che fino allo scorso anno interessava il 64% degli adolescenti\) e tale condizione, nel 46% dei casi genera ansia, rabbia e fastidio. Questo fenomeno è meno diffuso tra i ragazzi più piccoli, tra gli 11 e i 14 anni, che si fermano ancora al 60% e solo il 32% sperimenta alti livelli di ansia e preoccupazione"](#).

Spesso il trascorrere del tempo online, in termini disfunzionali, è scandito dal gioco virtuale che può anche assumere forme di Dipendenza dal gioco online (Net gaming addiction o Internet Gaming Addiction) inserito all'interno del Manuale Diagnostico Statistico dei Disturbi Mentali (DSM 5). Da specificare che la dipendenza qui si realizza quando c'è un abuso, ossia un utilizzo continuativo e sistematico della Rete al fine di giocare impegnando la maggior parte delle giornate, con la conseguente sottrazione del tempo alle altre attività quotidiane del minore.

In particolare, [sei sono le componenti che a livello bio-psico-sociale possono portare ad una vera e propria dipendenza](#). Di seguito i sintomi che devono essere presenti (per un arco di tempo di almeno un anno):

1. il giocatore è assorbito totalmente dal gioco;
2. il giocatore è preoccupato e ossessionato dal gioco (si veda Lancini M., Il ritiro sociale negli adolescenti, Raffaello Cortina Ed., Milano, 2019);
3. il gioco consente alla persona di sfuggire alla realtà con la sperimentazione di emozioni più piacevoli;
4. il giocatore manifesta sempre di più l'impulso di giocare e di sperimentare emozioni positive;
5. il giocatore sente di dover dedicare più tempo ai giochi;
6. il giocatore se non può giocare manifesta ansia, depressione e irritabilità;
7. può emergere un ritiro sociale (si veda il punto 3);
8. il giocatore, anche se comprende la gravità della situazione e sospende di giocare comunque non riesce a interrompere del tutto;
9. il giocatore mente agli altri sull'utilizzo che fa dei giochi on line;
10. il giocatore ha perso o mette a rischio relazioni o opportunità a causa dei giochi su Internet o ha perso interesse verso attività nella vita reale.

Anche in questo caso, la scuola ha la possibilità di fare formazione e di indicare strategie per un uso più consapevole delle tecnologie per favorire il "benessere digitale", cioè la capacità di creare e mantenere una relazione sana con la tecnologia.

La tecnologia infatti ha modificato gli ambienti che viviamo e ha un impatto sulla qualità della vita. Gli [elementi che contribuiscono al benessere digitale sono](#):

- la ricerca di equilibrio nelle relazioni anche online
- l'uso degli strumenti digitali per il raggiungimento di obiettivi personali
- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile
- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche)

Questo è un argomento trasversale, se ne può parlare quando si parla di cittadinanza digitale, di cyberbullismo, di uso integrativo e non sostitutivo dei dispositivi e della Rete; tanto più può essere utile dedicare al tema un momento specifico e riflettere con studenti e studentesse per fare in modo che la tecnologia sia strumento per raggiungere i propri obiettivi e non sia solo distrazione o addirittura ostacolo.

La scuola può insegnare molto da questo punto di vista se integra la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online.

Si potrebbe riflettere insieme su: come trascorri il tempo on line? Quando aggiunge valore alla tua vita e quando ti fa perdere tempo? Quale atteggiamento potrei cambiare quando sono online? Che ruolo ha e deve avere la tecnologia (internet o il gioco) nella mia vita?

Allo stesso modo quando parliamo di videogiochi, dobbiamo pensarli non in termini negativi ma di benessere digitale. Sono parte del mondo di studenti e studentesse. E, allora, riflettiamo insieme a ragazzi e ragazze su: quando sono una risorsa? Accedono a contenuti adeguati all'età? A che ora e per quanto tempo li usano? Diventa utile riflettere con i ragazzi e le ragazze rispetto all'uso della tecnologia in termini di qualità e tempo.

Se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi.

Ecco, allora, che si potrà giungere a delle regole condivise e alla stipula di un "patto" d'aula e si potranno proporre delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d'aula.

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 medialità 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.

“Secondo una [recente ricerca di Skuola.net](#) per la Polizia di Stato - ricerca che ha coinvolto 6.500 ragazzi tra i 13 e i 18 anni - il 24% di loro ha scambiato almeno una volta immagini intime con il partner via chat o social (fenomeno conosciuto come sexting). Tra questi, il 15% ha subito la condivisione con terzi, senza consenso, di questo materiale. Il motivo più frequente, riportato dalle vittime? Un banale “scherzo” (49%), a dimostrazione di quanto possano essere sottovalutate le reali conseguenze di tale diffusione. Tra le altre motivazioni, il ricatto (11%) o la vendetta (7%): il revenge porn, pure presente, viene surclassato dalla leggerezza e dalla goliardia ma gli effetti sono drammaticamente gli stessi. La reazione più diffusa nella maggior parte dei casi è il silenzio: il 53% ha fatto finta di niente, il 31% non ha detto nulla per non essere giudicato”.

Il sexting (abbreviazione di sex - sesso e texting - messaggiare, inviare messaggi) indica l'invio e/o la ricezione di contenuti (video o immagini) sessualmente espliciti che ritraggono se stessi o gli altri.

[“Spesso sono realizzate con il telefonino, e vengono diffuse attraverso il cellulare \(tramite invio di mms o condivisione tramite bluetooth\) o attraverso siti, e-mail, chat. Spesso tali immagini o video, anche se inviate ad una stretta cerchia di persone, si diffondono in modo incontrollabile e possono creare seri problemi, sia personali che legali, alla persona ritratta. L'invio di foto che ritraggono minorenni al di sotto dei 18 anni in pose sessualmente esplicite configura, infatti, il reato di distribuzione di materiale pedopornografico”.](#)

I contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di “revenge porn” letteralmente “vendetta porno” fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte (la Legge 19 luglio 2019 n. 69, all'articolo 10 ha introdotto in Italia il reato di revenge porn, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti. Si veda l'articolo 612 ter del codice penale rubricato [“Diffusione illecita di immagini o video sessualmente espliciti”](#). Tra le caratteristiche del fenomeno vi sono principalmente:

- la fiducia tradita: chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo, inoltre, alla motivazione della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale);
- la pervasività con cui si diffondono i contenuti: in pochi istanti e attraverso una condivisione che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso a un numero esponenziale e infinito di persone e ad altrettante piattaforme differenti. Il contenuto, così, diventa facilmente modificabile, scaricabile e condivisibile e la sua trasmissione è incontrollabile;

- la persistenza del fenomeno: il materiale pubblicato online può permanervi per un tempo illimitato e potrebbe non essere mai definitivamente rimosso. Un contenuto ricevuto, infatti, può essere salvato, a sua volta re-inoltrato oppure condiviso su piattaforme diverse da quelle originarie e/o in epoche successive.

La consapevolezza, o comunque la sola idea di diffusione di contenuti personali, si replica nel tempo e può finire con il danneggiare, sia in termini psicologici che sociali, sia il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che hanno contribuito a diffonderla. Due agiti, quindi, che sono fra loro strettamente legati e che rappresentano veri e propri comportamenti criminali i quali hanno ripercussioni negative sulla vittima in termini di autostima, di credibilità, di reputazione sociale off e on line. A ciò si associano altri comportamenti a rischio, di tipo sessuale ma anche riferibili ad abuso di sostanze o di alcool.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/i e depressione.

L'Istituto nel tentativo di educare i propri alunni sulla pericolosità del sexting ha aderito a una campagna di Educazione Sociale dal titolo "Stop sexting and Revenge porn" promossa da Mete Onlus e patrocinata dall'Assessorato Regionale dell'Istruzione e della Formazione Professionale e dalla Presidenza dell'Assemblea Regionale Siciliana. Tale campagna si pone come obiettivo, attraverso la diffusione del Manifesto, la sensibilizzazione delle giovani generazioni al fine di contrastare la violenza contro le donne e l'educazione al sentimento.

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 problematica dell'adescamento online (come quella del sexting), quindi, si inquadra in uno scenario più ampio di scarsa educazione emotiva, sessuale e di assenza di competenza digitale, in riferimento al modo in cui i/le ragazzi/e vivono la propria sessualità e la propria immagine online, al loro desiderio di esprimersi e affermare se stessi.

Fondamentale quindi, come sappiamo, è portare avanti un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è).

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](#).

Se si è a conoscenza di tale tipologia di reato è possibile far riferimento alla: Polizia di Stato - Compartimento di Polizia postale e delle Comunicazioni; Polizia di Stato - Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri - Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato - Commissariato online.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/22).

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/lle

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.

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

Scegliere almeno 1 di queste azioni:

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.

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.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

- **Cyberbullismo:** è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online:** se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona 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 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.

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 fare 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:1.96.96).

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.

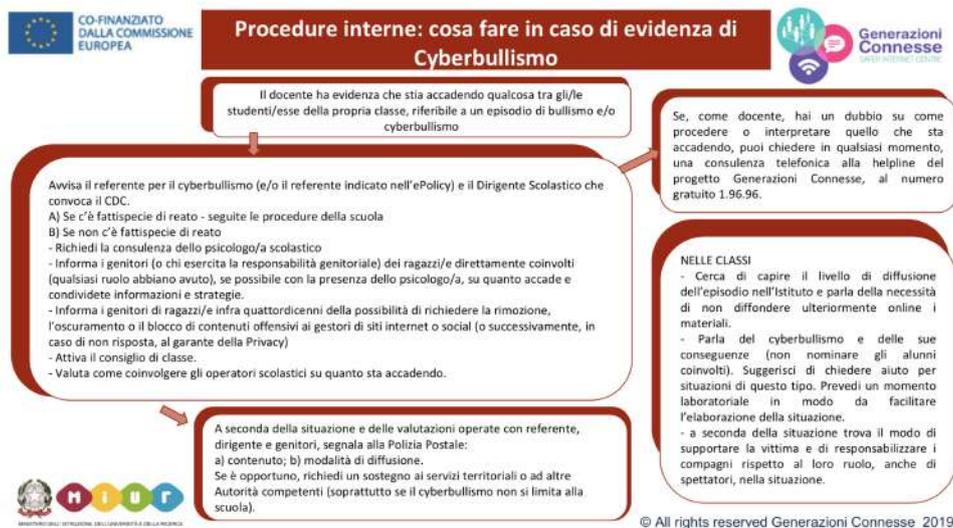
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all’utilizzo di Internet può presentare.

- **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?



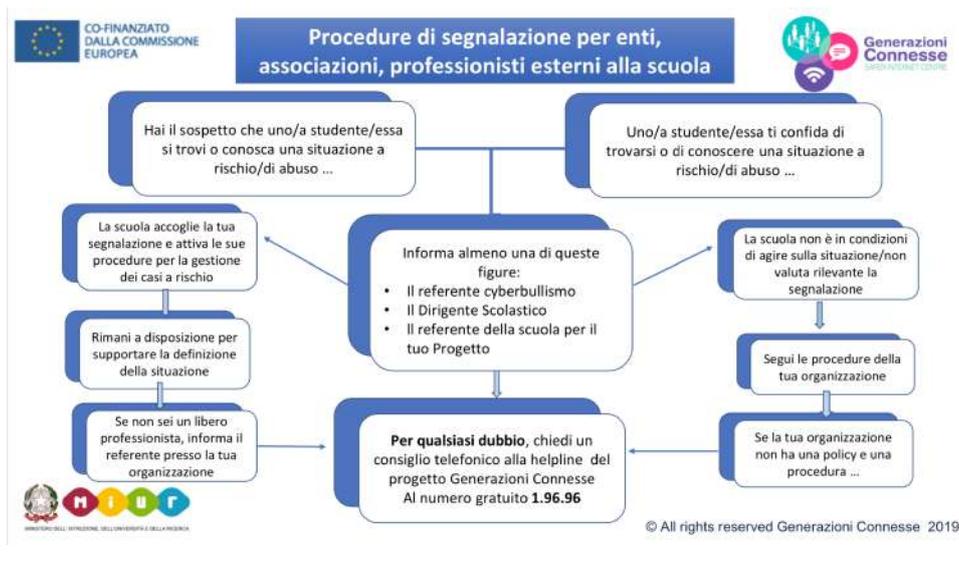
Procedure interne: cosa fare in caso di sexting?



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

Divulgazione delle procedure interne: cosa fare e a chi segnalare.

