# Documento di ePolicy

PZIC89200A

I.C. LAVELLO 1 VILLAREALE

PIAZZA MATTEOTTI 13/1 - 85024 - LAVELLO - POTENZA (PZ)

AURELIA ANTONIETTA BAVUSO

# 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



# 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.

# *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.

Di seguito si indicano i ruoli e le responsabilità degli utenti coinvolti.

| **Ruoli** | **Responsabilità** |
|---|---|
| **DIRIGENTE SCOLASTICO (e collaboratori)** | • garantisce la tutela legale della privacy, degli alunni e degli altri utenti adulti al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui ha accesso;<br>• garantisce al personale docente e ATA la formazione e l'aggiornamento sulle TIC;<br>• si assicura che esista un sistema di monitoraggio che garantisca la sicurezza on line. |
| **ANIMATORE DIGITALE** | • organizza momenti di condivisione con alunni e genitori di buone pratiche didattiche legate all'utilizzo delle TIC;<br>• stimola la messa in atto di laboratori con i docenti al fine di incentivare l'utilizzo delle TIC;<br>• monitora le problematiche che emergono nell'utilizzo delle TIC e della rete. |

| | |
|---|---|
| **DOCENTI** | • provvedono alla formazione e all'aggiornamento sulle TIC;<br>• si occupano di fornire indicazioni agli alunni sul corretto utilizzo degli strumenti informatici e della rete per l'uso scolastico ed extrascolatico;<br>• illustrano agli alunni e poi ai genitori nel corso delle assemblee di classe, le regole contenute nel presente documento;<br>• segnalano al DS e ai genitori comportamenti non corretti degli alunni nell'utilizzo della rete e degli strumenti informatici (pc, tablet, cellulari).<br><br>**Durante l'attività didattica ogni docente può avvalersi degli strumenti a disposizione e deve:**<br><br>• custodire la segretezza delle credenziali d'accesso al registro elettronico;<br>• non divulgare agli alunni le credenziali di accesso alla rete WIFI riservata ai docenti;<br>• installare e utilizzare solo software autorizzati;<br>• lasciare invariate le impostazioni dei dispositivi della scuola;<br>• compilare il registro d'uso per garantire la tracciabilità delle attività e il mantenimento in buono stato della strumentazione tecnologica utilizzata, segnalando celermente eventuali malfunzionamenti ai responsabili, secondo le modalità previste;<br>• non salvare sui dispositivi utilizzati file contenenti dati personali e/o sensibili;<br>• non memorizzare credenziali, email, file personali sui dispositivi;<br>• premurarsi che l'accesso degli alunni alla Rete avvenga sempre sotto la propria supervisione, informarli sui rischi cui sono potenzialmente esposti e sul corretto uso della Rete (motori di ricerca, piattaforme online, classi virtuali);<br>• visionare preventivamente i siti da proporre, verificandone accuratamente la sicurezza e il rispetto dei diritti di proprietà intellettuale;<br>• guidare gli alunni nelle ricerche online: fornire obiettivi chiari, proporre indirizzi web, parole chiave per la ricerca, prediligendo siti istituzionali, creati ad hoc per la didattica; vigilare, durante la navigazione, che tutti usino in modo corretto la Rete;<br>• segnalare ai responsabili l'uso di siti internet non compatibili con la politica educativa dell'Istituto. |
| **REFERENTE BULLISMO E CYBER BULLISMO (articolo 1, comma 1, del disegno di legge del Senato n. 1261 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyber bullismo")** | • provvede alla sua formazione personale come previsto dal disegno di legge;<br>• incentiva e propone corsi di formazione e aggiornamento a tutti i colleghi dell'istituto;<br>• promuove momenti di condivisione e discussione con gli altri docenti;<br>• si occupa di raccogliere le segnalazioni e di condividerle con il DS;<br>• insieme al DS, ai colleghi del C.d.C. e ai genitori, provvede alla progettazione e alla messa in atto di strategie educative indirizzate al singolo, alla classe o all'intero corpo studentesco. |

| | |
|---|---|
| **ALUNNI** | • si impegnano a leggere, comprendere e aderire a questa policy;<br>• utilizzano gli strumenti informatici seguendo le indicazioni e le norme di comportamento fornite dai docenti e presenti in questo documento;<br>• si impegnano a mantenere condotte rispettose e disciplinate nel corso della navigazione a scuola e a casa;<br>• si impegnano ad accedere al laboratorio di informatica solo se accompagnati da docenti e seguire le indicazioni fornite. in merito all'utilizzo delle TIC;<br>• si impegnano ad accedere agli ambienti di lavoro con le proprie credenziali, senza divulgarle, e archiviare i propri file in modo ordinato, così da essere facilmente rintracciabili, all'interno di cartelle dedicate o su supporto esterno preventivamente autorizzato;<br>• si impegnano ad accedere alla Rete solo in presenza e previa autorizzazione del docente responsabile dell'attività;<br>• si impegnano ad utilizzare la strumentazione della scuola solo per scopi didattici e non personali;<br>• si impegnano a lasciare immutata la configurazione di sistema dei dispositivi;<br>• si impegnano a chiudere correttamente la propria sessione di lavoro.<br><br>Inoltre per specifiche attività didattiche organizzate dal docente di classe è consentito l'uso a scuola di dispositivi personali (BYOD), in tutte le attività didattiche che comportano l'uso delle nuove tecnologie.<br>È consentita la registrazione delle lezioni a tutti gli studenti, previa autorizzazione scritta del docente, consegnata agli atti della scuola. |
| **GENITORI** | • si impegnano a leggere, comprendere e aderire a questa policy;<br>• si impegnano a sostenere la linea di condotta adottata dalla scuola e presente nel documento di e-policy;<br>• si impegnano a comunicare alla figura referente individuata e/o direttamente al DS di atti di cyberbullismo; grooming, sexting avvenuti a scuola;<br>• si impegnano a controllare con regolarità il registro elettronico e il sito istituzionale dell'Istituto;<br>• si impegnano a monitorare il modo in cui i figli usano la tecnologia e guidarli verso un comportamento responsabile e sicuro;<br>• collaborare con la scuola per la realizzazione di attività e progetti che prevedono l'utilizzo di dispositivi personali (BYOD);<br>• si impegnano a confrontarsi con i docenti e/o dirigente scolastico dell'Istituto se dovessero sorgere preoccupazioni riguardo l'uso delle nuove tecnologie da parte del figlio;<br>• concordano con i docenti e/o con il DS le linee educative da intraprendere nel caso di segnalazione. |

## 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).

Le organizzazioni, le associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, alla realizzazione di progetti ed attività educative nel nostro Istituto dovranno prendere atto di quanto stilato nel documento di E-policy e sottoscrivere un'informativa sintetica del documento in questione allegata al contratto.

## 1.4 - Condivisione e comunicazione dell’ePolicy all’intera comunità scolastica

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

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

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

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

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

Il documento di ePolicy è condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. Nello specifico il testo sarà condiviso con:

- **studenti e studentesse** per 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;
- **personale scolastico** per poter orientare tutte le figure sui temi in oggetto, a partire da un uso corretto dei dispostivi e della Rete in linea anche con il codice di comportamento dei pubblici dipendenti;
- **i 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.

**GESTIONE DELLE INFRAZIONI DEGLI ALUNNI**

Le potenziali infrazioni in cui potrebbero incorrere gli alunni, relativamente alla fascia di età considerata, nell'utilizzo delle tecnologie digitali e di internet durante la didattica sono le seguenti:

- uso della RETE per giudicare, infastidire, offendere, denigrare, impedire a qualcuno di esprimersi o partecipare;
- esprimersi in modo volgare usando il turpiloquio;
- invio incauto o senza permesso di foto o altri dati personali (indirizzo di casa, numero di telefono);
- condivisione online di immagini o video di compagni/e e del personale scolastico senza il loro esplicito consenso o che li ritraggono in pose offensive e denigratorie;
- condivisione di immagini intime e a sfondo sessuale;
- comunicazione incauta e senza permesso con sconosciuti;
- collegameti a siti web non adeguati e non indicati dai docenti.

L'azione educativa prevista per gli alunni deve essere rapportata alla fascia di età e al livello di sviluppo e maturazione personale. Infatti in alcuni casi i comportamenti sanzionabili sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, di cui gli educatori devono tenere conto per il raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno. Pertanto sono previsti interventi graduali in base all'età e alla gravità delle violazioni:

- richiamo verbale;
- richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività in atto);
- richiamo scritto con annotazione sul diario e sul registro;
- convocazione dei genitori da parte dell'insegnante;
- convocazione dei genitori da parte del Dirigente Scolastico.

Contestualmente sono previsti interventi educativi di rinforzo tesi a corrergreggere e riparare i disagi causati, a ri-definire le regole sociali di convivenza, di prevenzione e gestione positiva dei conflitti, di pro-socialità, di conoscenza e gestione delle emozioni. E' inoltre importante intervenire su tutto il contesto classe con attività specifiche educative e di sensibilizzazione.

**GESTIONE DELLE INFRAZIONI DEL PERSONALE SCOLASTICO**

Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet sono diverse e alcune possono determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli allievi:

- utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di docenza o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiale non idoneo;
- utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- trattamento dei dati personali e dei dati sensibili degli alunni non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;

- diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- carente istruzione preventiva degli alunni sull'uso corretto e responsabile delle TIC e di internet;
- vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili.

Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a Internet, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone una copia per eventuali successive investigazioni. Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo, gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

**GESTIONE DELLE INFRAZIONI DEI GENITORI**

In considerazione dell'età degli alunni e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico. Le situazioni familiari meno favorevoli sono:

- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai;
- una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio;
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone;
- un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei;
- un utilizzo del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria indirizzi o contenuti non idonei.

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

## 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.

Il presente documento di e-policy, è parte integrante del P.T.O.F..

## 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.

L'aggiornamento del documento di e-Policy sarà curato dal docente Referente di Istituto per la prevenzione e il contrasto del bullismo e cyberbullismo, in qualità di coordinatore del gruppo di lavoro del presente documento.

## Il nostro piano d'azioni

### Azioni da svolgere entro un'annualità scolastica:

- Organizzare di eventi di presentazione del progetto Generazioni Connesse rivolto agli studenti, ai docenti e ai genitori.

### Azioni da svolgere nei prossimi 3 anni:

- Monitoraggio annuale rivolto ai docenti, agli studenti e ai genitori,

finalizzato all'eventuale aggiornamento dell'ePolicy.

- Organizzare incontri, durante le attività di Educazione Civica, per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.

# Capitolo 2 - Formazione e curricolo

## *2.1. Curricolo sulle competenze digitali per gli studenti*

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

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

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

Le finalità del Curricolo verticale saranno le seguenti:

- favorire la conoscenza dello strumento informatico a scopo didattico;
- sostenere l'alfabetizzazione informatica;
- favorire la trasversalità delle discipline;
- facilitare il processo di apprendimento;
- favorire il processo di inclusione;
- fornire nuovi strumenti a supporto dell'attività didattica;
- promuovere situazioni collaborative di lavoro e di studio;
- promuovere e sviluppare il pensiero computazionale; • sviluppare creatività e capacità di lavorare in gruppo;
- promuovere azioni di cittadinanza attiva;
- utilizzare in modo critico, consapevole e collaborativo la tecnologia.

Le competenze digitali saranno declinate secondo le cinque aree del quadro di riferimento DIGCOMP (Quadro comune di riferimento europeo per le competenze digitali).

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 individuale e le licenze.
4. SICUREZZA: protezione personale, protezione dei dati, protezione dell'identità digitale, misure di sicurezza, uso sicuro e sostenibile.
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 i problemi tecnici, aggiornare la propria competenza e quella altrui.

---

## *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.

Un buon numero di docenti ha già partecipato a corsi di formazione specifici sia nell'ambito di piani nazionali, sia nell'ambito di iniziative organizzate dall'istituzione stessa relativi all'uso della Piattaforma Microsoft Office 365. Il corpo docente possiede generalmente una buona base di competenze e nel caso delle figure di sistema, anche di carattere specialistico. Il personale è disponibile ad aggiornarsi per mantenere al passo la propria formazione, in rapporto al rinnovo della dotazione multimediale e al

continuo sviluppo delle nuove tecnologie.

---

## 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.

I momenti di formazione ed aggiornamento saranno formulati secondo un'analisi del fabbisogno formativo del corpo docente sull'utilizzo ed integrazione delle TIC nella didattica e sull'uso consapevole e sicuro di Internet e sui rischi della rete.

Inoltre, il percorso di formazione specifica dei docenti non può essere mai considerato esaustivo, ma deve essere permanente in relazione all'evoluzione rapida delle tecnologie e delle modalità di comunicazione. Potrà prevedere momenti di autoaggiornamento e di formazione personale o collettiva.

La scuola si impegna a supportare la formazione attraverso corsi interni o esterni, mediante seminari, conferenze e dibattiti. Non si escluderà la formazione a distanza né la partecipazione ad iniziative al di fuori della programmazione d'Istituto.

---

## 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.

L'Istituto, inoltre, attiverà iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine saranno previsti incontri fra docenti e/o esperti e genitori sui temi oggetto della Policy per la diffusione del materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati (Generazioni Connesse) e dalle forze dell'ordine. Sul sito della scuola, inoltre, sarà pubblicato il presente documento per la divulgazione delle informazioni e delle procedure contenute, per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'Istituto e per prevenire i rischi legati ad un utilizzo scorretto di Internet.

## *Il nostro piano d'azioni*

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

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare e promuovere, se necessario, per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie 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.

In merito alla protezione dei dati personali, si fa riferimento a quanto previsto dal Decreto Legislativo del 30 giugno 2003, n.196 (cosiddetto Codice della Privacy), integrato dal D. Lgs. 10 agosto 2018, n. 101, e dal GDPR (General Data Protection Regulation) n. 679 del 2016.

All'atto dell'iscrizione vengono fornite ai genitori una informativa e una richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori, come ad esempio l'utilizzo di fotografie, video o altri materiali audiovisivi contenenti l'immagine e/o il nome del proprio figlio/a all'interno di attività educative e didattiche per scopi documentativi, formativi e informativi, durante gli anni di frequenza della scuola. A tale proposito si evidenzia che le immagini e le riprese audiovideo realizzate dalla scuola, nonché gli elaborati prodotti dagli studenti durante le attività scolastiche, potranno essere utilizzati esclusivamente per documentare e divulgare le attività della scuola tramite il sito Internet di Istituto.

---

# *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.

ACCESSO AD INTERNET: FILTRI, ANTIVIRUS E SULLA NAVIGAZIONE

L'accesso ad internet è differenziato per gli uffici di segreteria e per la didattica. le due linee di accesso sono fisicamente separate.

L’accesso ad internet, per uso didattico, è possibile in tutti i plessi dell’Istituto. La linea LAN fornisce l’accesso internet in tutte le aule e i laboratori e la rete WIFI copre tutti gli edifici scolastici.

L’accesso alla RETE WIFI dell’intero edificio Matteotti (Plesso Scuola Primaria e Plesso Sc. Sec. di I Grado) è gestito da un sistema di CAPTIVE PORTAL, pertanto tutte le utenze sono registrate ed autorizzate. Nella Scuola dell’Infanzia e nel Plesso S. Anna, l’accesso avviene tramite password di sistema aggiornate periodicamente e consegnate solo ai docenti e al personale scolastico.

I computer portatili collocati nelle aule accedono ad internet attraverso rete WIFI. Nei laboratori informatici sono presenti computer portatili e fissi. I Computer fissi dei Laboratori accedono alla RETE attraverso rete LAN. Tutti i computer presenti nella scuola hanno installato un antivirus. Gli studenti non possono accedere con i loro dispositivi alla rete internet della scuola. Gli studenti possono accedere alla RETE didattica dell’Istituto, solo con device della Scuola e in occasione di attività didattiche che si svolgono prevalentemente nei laboratori informatici e nelle cl@asse 2.0, sempre guidati dall’insegnante.

FIREWALL

Tutta la rete didattica, sia la linea LAN che la rete WIFI, in tutti i plessi dell’Istituto è gestita da RouterBoard Mikrotik in cui sono state configurate le seguenti regole di FIREWALL:

- DNS NORTON SECURITY

| | | |
|---|---|---|
| Politica 3: Sicurezza + Pornografia + Altro | • 199.85.126.30<br>• 199.85.127.30 | Ideale per le famiglie con bambini piccoli. Oltre a bloccare siti non sicuri e pornografici, questa politica blocca anche l'accesso a siti con contenuti per adulti o relativi ad aborto, alcool, crimine, culti, droghe, gioco d'azzardo, odio, orientamenti sessuali, suicidio, tabacco e violenza. |

- DNS STATICI per attivare SECURE SEARCH sui motori di ricerca principali (Google, Bing, Youtube)

GESTIONE ACCESSI (PASSWORD, BACKUP, ECC…)

I computer portatili presenti nelle aule non richiedono una password di accesso per l'accensione. Ogni docente è quindi tenuto ad un controllo della strumentazione in aula poiché l'uso del dispositivo è permesso agli alunni solo su autorizzazione dell'insegnante. Ogni docente accede al registro elettronico attraverso una password personale che non può essere comunicata a terzi, né agli alunni.

E-MAIL E REGISTRO ELETTRONICO

Ogni docente possiede una propria mail e credenziali personali per l'accesso al registro elettronico. Gli account sono strettamente personali, per cui ogni utente dovrà avere cura di disconnettere il proprio accesso al termine del suo utilizzo.

SITO WEB DELLA SCUOLA

Per il sito web della scuola è stato adottato il protocollo HTTPS per la comunicazione su Internet che protegge l'integrità e la riservatezza dei dati scambiati tra i computer e i siti. Il sito istituzionale è gestito dal personale amministrativo, l'unico che accede ad aree riservate, a tutti gli altri utenti, pertanto, è permessa la sola visualizzazione.

Sul sito è possibile trovare regolamenti, materiali didattici, pubblicizzazione di eventi, documentazione di attività curricolari ed extracurricolari svolte. Pulsanti attivi permettono l'accesso a link di interesse tra cui il Registro Elettronico. Tutti i contenuti del settore didattico sono pubblicati direttamente e sotto supervisione del Referente Scolastico, che ne valuta con il Dirigente scolastico la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc.

Il sito è aggiornato periodicamente dal personale amministrativo e dal Referente Scolastico.

SOCIAL NETWORK

L'utilizzo dei social network nella didattica deve essere contestualizzato ad attività specifiche.

---

# 3.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

La comunicazione interna ed esterna del nostro Istituto è gestita attraverso:

- il sito web https://ics1lavello.edu.it;
- canale telegram per la notifica delle notizie pubblicate sul sito web ai docenti e alle famiglie;
- comunicazione della segreteria didattica di e-mail a tutto il personale scolastico;
- registro elettronico ARGO;
- piattaforma Microsoft Office 365 per la gestione delle classi virtuali e la partecipazione a forms indirizzati al personale, agli studenti e alle famiglie.

Il registro elettronico consente una comunicazione chiara e immediata con le famiglie relativamente a:

- andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari);
- risultati scolastici (voti, documenti di valutazione);
- udienze (prenotazioni colloqui individuali);
- comunicazione varie (comunicazioni di classe, comunicazioni personali).

Tutte le comunicazioni scuola-famiglia contenenti dati sensibili sono visibili da parte della famiglia dell'alunno interessato e non dal resto della classe. Solo il D.S. e i docenti del C.d.C. possono avere accesso a tali informazioni.

---

# 3.4 - Strumentazione personale

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

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

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

**NORME GENERALI DELL'USO DI DEVICE MOBILI PERSONALI A SCUOLA**

Il personale, gli studenti e i genitori o i visitatori che portano nell'Istituto i device di loro proprietà sono responsabili del proprio dispositivo e lo portano nell'Istituto a proprio rischio.

Se il device si rompe, viene smarrito, viene danneggiato, vengono persi dei dati ecc., la scuola non deve essere considerata responsabile della sicurezza di tali dispositivi/dati né deve farsi carico di eventuali risarcimenti.

L'istituto consiglia vivamente a tutti gli studenti di non portare telefoni cellulari e dispositivi mobili personali a scuola se non espressamente richiesto dagli insegnanti.

Se uno studente viola questa policy, il dispositivo verrà in tutti i casi trattenuto e lo si terrà in un luogo sicuro in ufficio di segreteria informando nell'immediatezza la famiglia. I dispositivi mobili saranno rilasciati solo ai genitori/tutore con delega.

Telefoni e dispositivi non devono essere mai usati durante gli esami o prove nazionali. Questo può anche portare all'esclusione dall'esame stesso.

Gli studenti sono responsabili della custodia del loro numero telefonico che non deve essere divulgato o gli ID/password personali. I ragazzi saranno guidati ad usare in modo appropriato e sicuro i loro smartphone/personal device e saranno istruiti sui limiti e le conseguenze di comportamenti non adeguati/non accettati.

L'uso di mobile device non è consentito per ricevere/effettuare chiamate, SMS o altro tipo di messaggistica, giocare, ecc.

Per quanto riguarda uscite, visite guidate e viaggi di istruzione, l'uso può essere

consentito, se autorizzato dal docente, al di fuori dei momenti dedicati a visite guidate e attività legate all'aspetto didattico dell'uscita.

La comunicazione con le famiglie, per qualsiasi urgenza, è sempre garantita attraverso il telefono della scuola.

Utilizzo delle funzioni che possono avere una rilevanza e un impiego nella didattica

In questo caso l'uso di smartphone, tablet e altri dispositivi mobili personali, è consentito:

- I dispositivi mobili personali verranno utilizzati unicamente durante le lezioni o il tempo scuola formale solo come parte di un'attività curriculare, secondo le modalità prescritte dall'insegnante e con esclusiva finalità didattica. Al termine dell'attività che prevede l'utilizzo del dispositivo, si applicheranno le norme di cui sopra.
- I ragazzi devono chiedere l'autorizzazione prima di caricare/postare o condividere fotografie, video, registrazione audio o qualsiasi altra informazione che riguarda se e anche altre persone.

## *Il nostro piano d'azioni*

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

**Scegliere almeno 1 di queste azioni:**

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse, dei docenti e del personale ATA.
- formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte deglistudenti e delle studentesse, dei docenti e del personale ATA.
- formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

## *4.1 - Sensibilizzazione e Prevenzione*

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

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

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

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

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

Nell'ottica della prevenzione l'Istituto si prefigge come obiettivo quello di fornire all'utenza le competenze necessarie al fine di tenere comportamenti responsabili e corretti per un uso corretto e responsabile nella fruizione delle TIC e della Rete. A tal fine fondamentali sono le seguenti strategie:

- avvio di percorsi di formazione per un uso consapevole delle TIC rivolti agli insegnanti nel corso dell'anno scolastico;
- coinvolgimento dei genitori come partner educativi nei percorsi di formazione che riguardano gli studenti;
- attuare, eventualmente in collaborazione con esperti esterni, incontri per presentare a tutte le componenti della comunità scolastica:
    - modalità corrette di fruizione del Web,
    - tutela dei minori su Internet e sui social network,
    - prevenzione e contrasto del fenomeno del cyberbullismo
    - uso responsabile del web;
- informare sulle problematiche psico-pedagogiche correlate all'uso della Rete;
- controllo (una tantum e/o all'evenienza di episodi dubbi) del sistema informatico (cronologia, cookies, ecc.) da parte dei responsabili;
- aggiornamento periodico delle regole firewall degli apparati che forniscono accessi alla rete;
- aggiornamento periodico del software antivirus e scansione delle macchine in caso di sospetta presenza di virus.

---

# *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).

Si definiscono "bullismo" tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o a volte un piccolo gruppo). Si tratta, pertanto, di una serie di comportamenti ripetuti nel tempo. Quando queste vessazioni vengono fatte online, diventano "cyberbullismo". Il cyberbullismo presenta le seguenti caratteristiche:

- **è invasivo**: il bullo può raggiungere la sua vittima in qualsiasi momento e in qualunque luogo;
- **è un fenomeno persistente**: il materiale messo online vi può rimanere per molto tempo;
- **ha una platea potenzialmente infinita**: le persone che possono assistere agli atti di cyberbullismo sono potenzialmente illimitate.

A seconda dei casi, si potranno adottare azioni di prevenzione universale, selettiva e indicata

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. Relativamente all'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.

---

# *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.

Relativamente all' Hate Speech, le azioni di prevenzione devono tendere a valorizzare la dimensione relazionale e a fornire ai più giovani 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; bisogna promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network; bisogna favorire una presa di parola consapevole e costruttiva da parte dei giovani.

Inoltre, l'Istituto si potrà avvalere di consulenti/esperti esterni per organizzare incontri formativi rivolti a docenti, genitori ed alunni (Carabinieri, Polizia Postale, equipe Formazione Territoriale del MIUR, associazioni del Territorio preposte allo scopo...).

---

# *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?*

Sarà fatta informazione e formazione sul fatto che la dipendenza da internet e il gioco online rappresentano una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito a insaputa di altri) rappresenta un vero e proprio illecito.

Le tecnologie e il gioco online rendono l'apprendimento accattivante, motivante e divertente, quindi il riconoscimento, la condivisione e il rispetto di alcune regole fondamentali si pone come obiettivo necessario per poter ricorrere a queste risorse.

---

# *4.5 - Sexting*

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

Il nostro Istituto, attraverso le attività di formazione, intende sensibilizzare e prevenire fenomeni legati all'uso inconsapevole delle TIC e dei social, tra i quali anche il sexting.

A tal proposito, saranno promossi i servizi offerti da Generazioni Connesse per la formazione e l'informazione ai genitori e al personale docente su tali problematiche, oltre che sulla normativa vigente.

---

# *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.

Al fine di prevenire casi di adescamento online è opportuno accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli emotivamente più sicuri e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato.

Fondamentale quindi, 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).

Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere, ad esempio, all'adescatore. È importante che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove. Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video…).

L'adescamento, inoltre, può essere una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.

---

# *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.**

Il nostro Istituto, attraverso le attività di formazione, intende sensibilizzare e prevenire fenomeni legati all'uso inconsapevole delle TIC e dei social, tra i quali anche la pedopornografia.

A tal proposito, saranno promossi i servizi offerti da Generazioni Connesse per la formazione e l'informazione ai genitori e al personale docente su tali problematiche, oltre che sulla normativa vigente.

## *Il nostro piano d'azioni*

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

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

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

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

# Capitolo 5 - Segnalazione e gestione dei casi

## 5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

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

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.

La scuola accoglierà e valuterà sempre segnalazioni relative a:

- **contenuti afferenti la violazione della privacy** (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);
- **contenuti afferenti all'aggressività o alla violenza** (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);
- **contenuti afferenti alla sessualità:** messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

---

# *5.2. - Come segnalare: quali strumenti e a chi*

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

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

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

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

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

---

## Strumenti a disposizione di studenti/esse

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

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Relativamente alla gestione dei casi, il nostro Istituto ha individuato una figura referente per il cyberbullismo.

In relazione al CASO A, è opportuno il coinvolgimento del Referente d'Istituto per il contrasto del bullismo e del cyberbullismo, al fine di valutare le possibili strategie d'intervento. Se si ravvisano gli estremi, viene informato il Dirigente scolastico unitamente al Consiglio di classe. Uno strumento utile per raccogliere informazioni può essere il diario di bordo (allegato alla presente e-Policy): il docente deve cercare di capire se gli episodi sono circoscritti al gruppo o se interessano l'intero Istituto. Operativamente è fondamentale coinvolgere tutti gli studenti e le studentesse, informandoli sui fenomeni e sulle caratteristiche degli stessi, suggerendo di chiedere aiuto se pensano di vivere situazioni, di subire atti identificabili come bullismo o cyberbullismo.

In relazione al CASO B, il docente deve condividere immediatamente quanto osservato con il Referente per il bullismo e il cyberbullismo, al fine di valutare insieme le possibili strategie di intervento. Sara necessario avvisare anche il Dirigente Scolastico che convocherà il Consiglio di classe.

Se non si ravvisano fattispecie di reato, sarà opportuno:

- informare i genitori (o chi esercita la responsabilità genitoriale) degli/delle studenti/studentesse direttamente coinvolti/e (qualsiasi ruolo abbiano avuto), se possibile con la presenza di professionisti dell'aiuto, per strategie condivise e modalità di supporto;
- creare momenti di confronto costruttivo in classe, con la presenza di figure

specialistiche territoriali;
- informare i genitori degli/delle studenti/studentesse infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy);
- convocare il consiglio di classe;
- valutare come coinvolgere gli operatori scolastici su quello che sta accadendo.

A seconda della situazione e delle valutazioni effettuate con Referente e il Team, il Dirigente scolastico valuterà se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali o ad altre autorità competenti.

---

# *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.

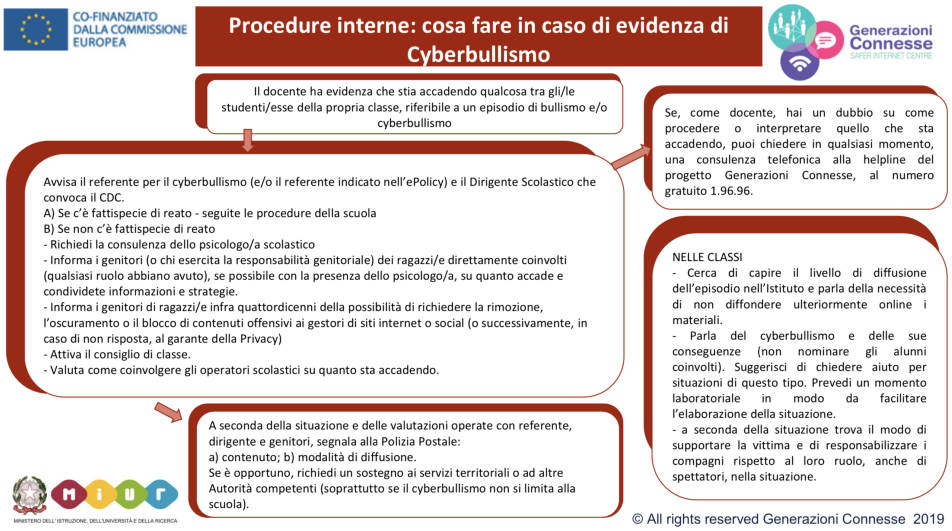
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare 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

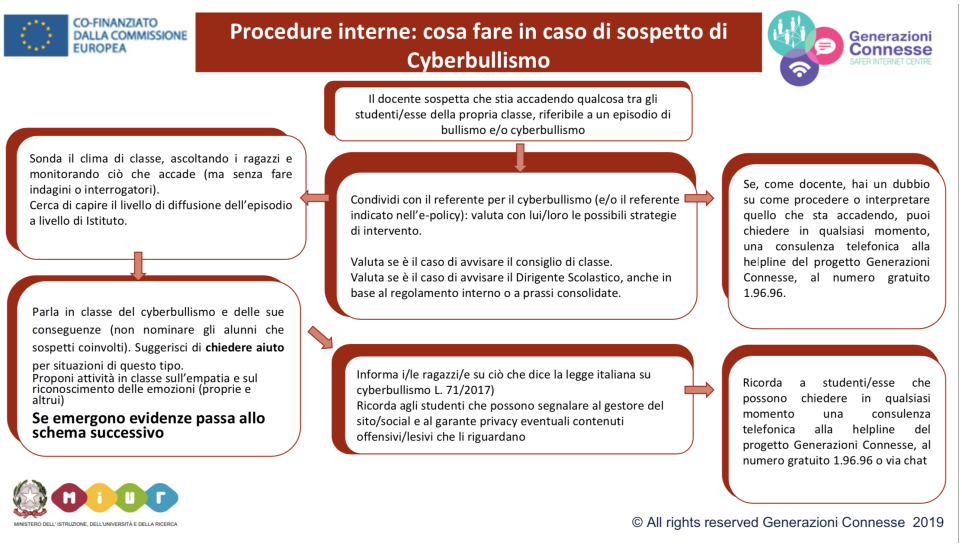
psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.

- **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.

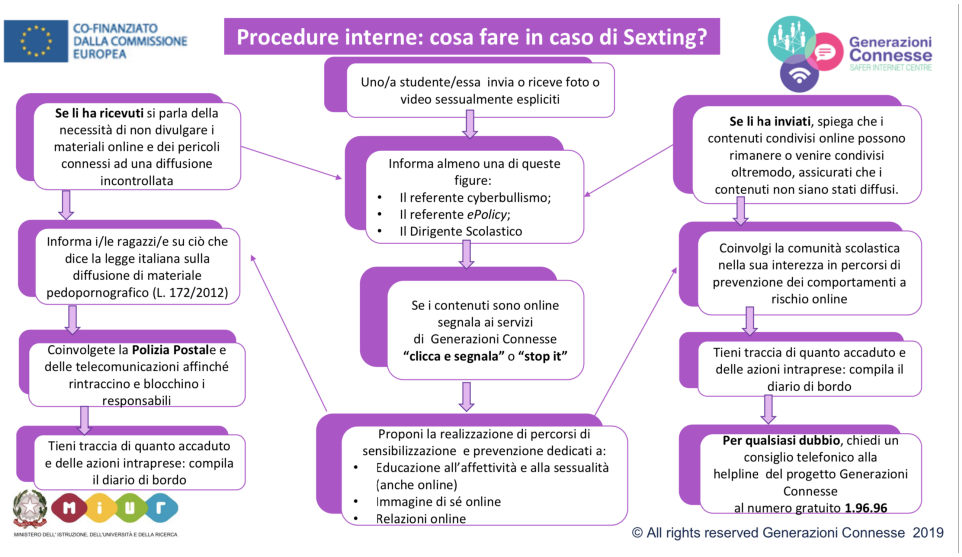
# *5.4. - Allegati con le procedure*

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

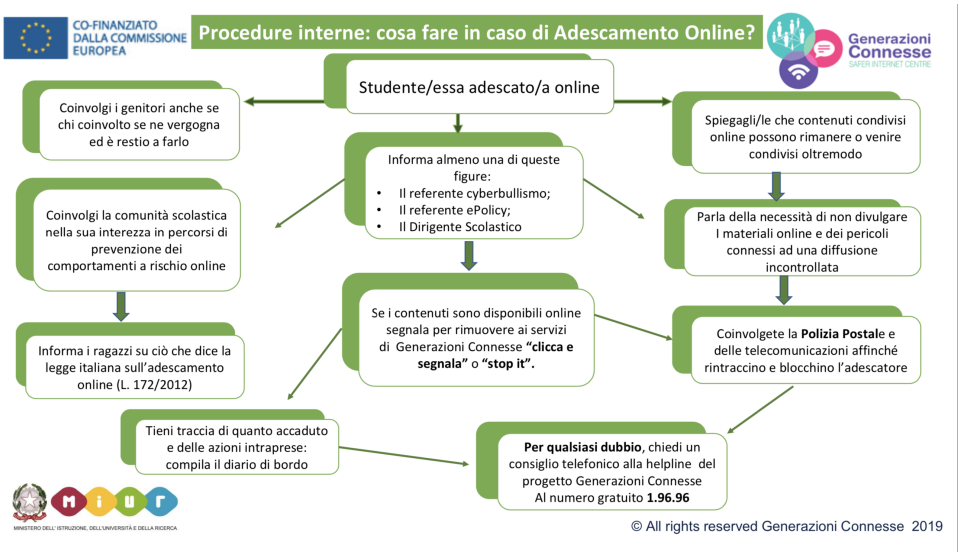




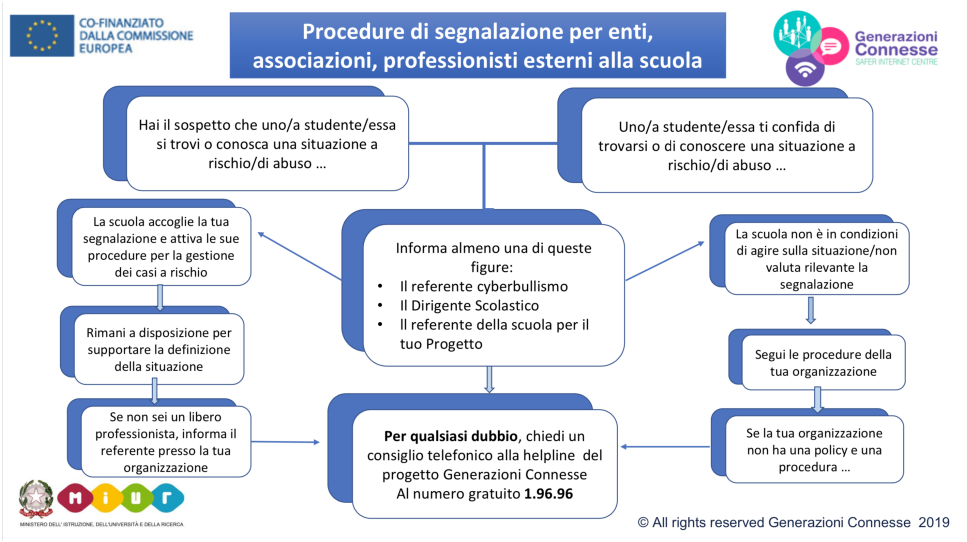

# Procedure interne: cosa fare in caso di sexting?




# 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*

BAVUSO AURELIA ANTONIETTA
30.06.2021 18:25:14
GMT+00:00