# Documento di ePolicy

CEIC8A9004

Istituto Comprensivo "Don Lorenzo Milani"

Viale delle Querce - 81100 - CASERTA - CASERTA (CE)

Francesco Mezzacapo

# 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.

La E-Policy, inoltre, potrà costiuire un supporto e fornire alcune linne guida per l'organizzazione dell'insegnamento di Cittadinanza digitale.

Nella stesura della E-Policy e nella definizione e attuazione delle procedure che questa prevede, oltre all'intera comunità scolastica, risultano principalmente coinvolti:

- Il Dirigente Scolastico, prof. Francesco Mezzacapo
- Il Team del Contrasto al bullismo e cyberbullismo, prof. Alessandro Maglione e prof.ssa Maria Carmina D'Angelo
- Il Primo Collaboratore del Dirigente Scolastico: prof.ssa Manuela Cortese
- L'Animatore Digitale: prof.ssa Lucia Cocco

---

# *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.

Il gruppo di lavoro per la stesura del documento di E-Policy è composto dal Dirigente Scolastico, prof. Francesco Mezzacapo, dal Team bullismo e cyberbullismo, prof. Alessandro Maglione e prof.ssa Maria Carmina D'Angelo, dal Primo Collaboratore del Dirigente Scolastico, prof.ssa Manuela Cortese e dall'Animatore Digitale, prof.ssa Lucia Cocco.

Il Dirigente Scolastico, anche con l'ausilio del Primo Collaboratore, si impegna per garantire la sicurezza, anche online, di tutti i membri della comunità scolastica. È 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; promuove la cultura della sicurezza online e, insieme all'Animatore Digitale e al docente referente sulle tematiche del bullismo/cyberbullismo, propone corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC. Inoltre, il Dirigente Scolastico ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

Il Team bullismo e cyberbullismo 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) può coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.

L'Animatore Digitale pubblica il presente documento sul sito e ne diffonde i contenuti, 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, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento anche allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica); monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola, e ha il compito di controllare che gli utenti autorizzati usino gli account forniti dall'Istituto e accedano alla Rete della scuola con apposita password solo per scopi istituzionali e consentiti (istruzione e formazione).

I Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Sono tenuti a integrare parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica. I docenti hanno il dovere di accompagnare e supportare 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) 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. È coinvolto nelle attività di formazione e autoformazione in tema di bullismo e cyberbullismo. Il personale ATA può essere coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

Gli Studenti e le Studentesse si impegnano, in relazione al proprio grado di maturità e consapevolezza raggiunta, a utilizzare al meglio gli strumenti e le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola devono imparare a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le; 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 e i Tutori legali, in continuità con l'Istituto scolastico, devono 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; hanno il dovere di 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. Sottoscrivendo il patto di corresponsabilità, si impegnano ad accettare e condividere quanto scritto nell'E-Policy dell'Istituto.

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

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

---

## *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).

Tutti gli operatori esterni presenti a qualsiasi titolo nella scuola dovranno attenersi alle norme previste dal presente documento di E-Policy dell'Istituto.

---

# 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.

***da compilare con le indicazioni contenute nella lezione***

---

# 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.

Educare alla "consapevolezza civica" verso un uso responsabile della rete è un dovere di tutta la comunità educante. Per questo motivo, accanto all'educazione verso la

competenza digitale, sarà premura della scuola introdurre preventivamente delle modalità formative, in caso utilizzo imprudente del web, nonché l'introduzione di strumenti educativi.

INFRAZIONI DEGLI ALUNNI

L'istituto, qualora si ravvisassero infrazioni all'E-policy nell'uso improprio delle TIC, da parte degli studenti, sarà tenuto ad introdurre delle misure per rinforzare i comportamenti corretti, e riparativi, degli eventuali danni causati. Gli interventi correttivi, ovviamente in rapporto all'anagrafe individuale e alla gravità dell'infrazione, sono previsti in relazione a:

- utilizzo di dati personali o foto senza permesso;
- condivisione di immagini a sfondo sessuale; collegamento a siti web non adatti all'anagrafe e non indicati dai docenti;
- furto di proprietà intellettuali (file o video musicali protetti da copyright);
- utilizzo della rete per offese, calunnie utilizzo di immagini o video che siano lesivi alla dignità persona

In ottemperanza a quanto disposto, i provvedimenti disciplinari da adottare sono i seguenti:

- richiamo verbale;
- informazione/comunicazione ufficiale ai genitori;
- sanzioni previste dal regolamento di istituto;
- convocazione dei genitori da parte del Dirigente Scolastico;
- sospensione dalle lezioni;
- in relazione alla gravità dell'infrazione, saranno eventualmente informate le autorità competenti.

INFRAZIONI DEL PERSONALE SCOLASTICO

Anche il personale docente, amministrativo, tecnico e ausiliario, può incorrere in infrazioni nell'utilizzo delle tecnologie digitali e del web; alcune di queste possono favorire conseguenze negative sull'utilizzo corretto delle TIC da parte degli alunni. Nello specifico sono da considerare non adeguati i seguenti comportamenti:

- utilizzo delle tecnologie e dei servizi della scuola, d'uso comune, non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- trattamento dei dati personali, comuni e 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'utilizzo responsabile delle TIC e del web;
- mancata vigilanza che può favorire anche un utilizzo non idoneo dei

dispositivi mobili tra alunni;
- insufficienti interventi di contrasto nelle situazioni critiche, volti a segnalare ai genitori, all'animatore digitale e al Dirigente Scolastico.

RESPONSABILITÀ GENITORIALE

In un clima di collaborazione fra scuola e famiglia, sarà rinforzata l'attenzione che i genitori, unitamente al corpo docente, dovranno riservare al monitoraggio riguardo l'utilizzo delle TIC da parte degli studenti; in questo l'animatore digitale fungerà da snodo di collegamento per fornire ai genitori indicazioni e consigli per un uso sicuro delle tecnologie digitali; per quanto riguarda i genitori dovranno garantire un controllo parentale verso siti web non certificati (giochi, scommesse, deep web), social media con pubblicazione foto e video che possano compromettere il benessere dei propri figli o dei loro compagni ed amici.

L'istituto scolastico sarà a fianco dei genitori anche per rappresentare le condizioni possibili che possono indurre a comportamenti scorretti. Di seguito alcune situazioni non favorevoli:

- piena autonomia concessa al figlio nell'uso del web e/o nell'utilizzo di devices e/o smartphone: su questo aspetto ricordiamo che i contenuti veicolati nel web da parte dei minori è ascrivibile ai genitori o chi per essi;
- disinteresse verso i devices in possesso dei figli, nonché i contenuti che possono essere veicolati; la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai;
- 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.

In relazione alle infrazioni legate all'utilizzo del web, tutta la comunità educante è tenuta a collaborare con il Dirigente Scolastico al fine di fornire ogni informazione utile per la valutazione del caso, e il necessario avvio del procedimento disciplinare. Ogni azione di carattere procedurale sarà regolata dalla normativa vigente. In relazione ad infrazioni promosse dagli alunni i genitori saranno convocati, informati sui fatti, e coinvolti nel concordare misure educative correttive, in base alla gravità delle violazioni rilevate.

---

# *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.

La E-Policy dell'Istituto Comprensivo "Don Milani" di Caserta fa riferimento e si armonizza con tutti gli altri regolamenti vigenti nell'Istituto, in particolare con PTOF, Regolamento interno e Patto di Corresponsabilità Educativa.

Le nuove tecnologie sono parte integrante del processo educativo; nel riconoscere questa evidenza il nostro istituto vuole, attraverso questo documento, dotarsi di un approccio programmatico volto a stabilire delle regole e misure di comportamento comuni, connesse in modo particolare all'uso consapevole e responsabile delle tecnologie informatiche.

Dal momento che la scuola tutta è orientata verso il concetto di "una comunità di pratiche", e la normativa vigente va in questa direzione, l'istituto intende con questo documento, rafforzare la conoscenza, nonché i principi che sottendono al rispetto delle regole, con finalità di formare cittadini responsabili e attivi, valorizzando i principi insiti nella Costituzione.

---

## *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 monitoraggio dell' implementazione della e-Policy verrà curato dai docenti referenti e da uno specifico gruppo di lavoro che si riunirà per incontri e confronti, al fine di discutere di prevenzione, di visionare materiali, aderire a progetti relativi alla sicurezza in Rete e qualora si verifichino cambiamenti significativi in riferimento all'uso delle tecnologie digitali all' interno della scuola, per rivedere, modificare e/o ampliare la E-Policy, in una logica di condivisione con tutto il corpo docente, il Dirigente Scolastico, la Funzione Strumentale per il PTOF e le famiglie.

---

# *Il nostro piano d'azioni*

## Azioni da svolgere entro un'annualità scolastica:

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

## Azioni da svolgere nei prossimi 3 anni:

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

# Capitolo 2 - Formazione e 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 competenze digitali, e la loro applicazione in ambito scolastico, non possono restare all'interno di uno specifico ambito disciplinare, ma devono diventare lo snodo di collegamento fra tutte le aree disciplinari coinvolte nel processo didattico-educativo. Gli studenti devono avere la possibilità di sviluppare gli approcci alle tecnologie digitali, al fine di consolidare la loro competenza in questo ambito, e la scuola, per quanto la riguarda, deve mettere in campo strategie educative per affrontare le nuove modalità di comunicazione ed interazione.

La sfida educativa, da parte della scuola, sta nel portare avanti dei percorsi che mirino a promuovere una consapevolezza digitale, verso l'uso responsabile delle nuove tecnologie.

Il nostro Istituto, partendo dalle indicazioni contenute nel PNSD, ha provveduto all'interno del suo curricolo delle competenze, di individuare dei framework

relativi alle tecnologie digitali che vanno a sostenere:

- L'informazione;
- La comunicazione;
- La sicurezza;
- L'attenzione ai contenuti veicolati;
- Protezione dei dati personali;
- Identificare i bisogni "informatici" espressi dalla comunità scolastica.

Pertanto, le azioni possibili che questo Istituto si propone di fare in merito alle competenze digitali sono:

- Programmare attività per l'uso consapevole delle TIC;
- Sviluppare consapevolezza riguardo l'impatto che possono avere le TIC nella vita delle persone;
- Rappresentare le conseguenze dei comportamenti scorretti all'interno della rete;
- Comprendere quale sia la modalità adeguata quando si utilizza l'ambiente on line;
- Discriminare nel modo adeguato e corretto contenuti e informazioni;
- Conoscere le conseguenze, anche disciplinari, quando si utilizza la rete in modo scorretto.

---

## *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.

La formazione continua è la base dell'attività educativa e didattica. Per questo il nostro Istituto, che comprende l'importanza della formazione, ritiene fondamentale che tutti i docenti siano formati ed aggiornati, in modo costante e adeguato sui rischi on line. I momenti formativi saranno programmati, in collaborazione con il personale dedicato

interno all'istituto (animatore digitale, referente bullismo e cyberbullismo), nonché con personale esterno qualificato, afferente alla rete di scuole, organismi del terzo settore e comparti istituzionali (forze dell'ordine). A fronte di ciò, consapevoli che la formazione non deve essere esaustiva ma bensì in relazione alla rapida evoluzione delle tecnologie digitali, il nostro Istituto dichiara l'intenzione di prevedere momenti di formazione personale e collettiva, anche a distanza.

---

# *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.

Dal momento che la rete risulta essere un tessuto sociale interattivo comune ad una vasta platea di persone, la scuola tutta, deve impegnarsi a programmare/progettare percorsi formativi, volti a sviluppare le competenze digitali; allo stesso tempo deve educare gli studenti e le studentesse ad un uso responsabile e consapevole del web. Oramai le competenze digitali sono contemplate dalle indicazioni nazionali ritenute anche dall'Unione Europea competenza chiave trasversale a tutte le discipline. Padroneggiare con abilità le nuove tecnologie digitali non significa solo avere "maggiori competenze" ma soprattutto essere responsabili dell'utilizzo che se ne può fare, nel rispetto degli altri e consapevoli dei rischi e pericoli che si possono causare.

Per sostenere questa visione l'Istituto ha investito sulla formazione digitale dei docenti, collegata con l'educazione alla cittadinanza e alla legalità, , che risultano essere aspetti fondamentali per chiunque utilizzi il web.

Nello specifico l'Istituto si propone l'intenzione di:

- Organizzare percorsi formativi rivolti a tutta la comunità educante;
- Attività e laboratori sulla sensibilizzazione verso l'utilizzo corretto consapevole e responsabile del web, anche in collaborazione con agenzie extrascolastiche e

rappresentanze delle istituzioni (Forze dell'ordine);
- Visione di documentari a tema, che rappresentino la gravità e la complessità dei rischi che si nascondono nella rete.

Nel sito dell'Istituto saranno consultabili da parte dei docenti, approcci teorici riguardo l'utilizzo consapevole del web; sarà altresì possibile dal sito istituzionale scolastico accedere al link di "Generazioni Connesse".

---

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

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

Il "Patto Educativo di Corresponsabilità" fra scuola e famiglia è il sigillo di una alleanza che non si esaurisce con la semplice modalità informativa, ma rappresenta una nuova modalità di coinvolgimento dell'intera comunità educante, che si sente partecipe nel processo formativo di ogni persona. Per il nostro Istituto la scuola e la famiglia sono i protagonisti dell'educazione dei ragazzi, e per questo, diventano alleati negli scambi comunicativi e relazionali. Anche il legislatore ha reso più esplicita questa necessita, prevedendo nell'art. 3 del D.P.R. n° 235 del 21/11/2007, quanto sia fondamentale instaurare un'alleanza forte fra istituzione scolastica e rete familiare. Nel patto di corresponsabilità sono richiamati i principali diritti e doveri che implicano necessari impegni e responsabilità.

Il patto di corresponsabilità, essendo l'espressione di una visione significativa ben più ampia di una realtà dinamica, si propone di essere il documento finalizzato alla costruzione di reti fra istituzione e ambito genitoriale, con tensione ai bisogni educativi di ogni studente. Per questo il nostro Istituto, sensibile ai bisogni di ogni alunno, si

propone di fornire un servizio attento e qualificato dal punto di vista didatticoeducativo, nonché culturale e relazionale, insistendo sulla capacità dell'Istituto, di perseguire obiettivi formativi significativi a favore della crescita armoniosa degli studenti. All'interno di questo patto di corresponsabilità, sarà data particolare importanza ai rischi connessi all'uso delle TIC, come sarà richiamata la responsabilità di tutti gli attori coinvolti nel processo educativo in relazione a ruoli e competenze. L'istituto sarà garante dell'informazione in tema di tecnologie digitali, previste dall'Epolicy, come sarà cura dello stesso aggiornare il Regolamento d'Istituto, il Patto di Corresponsabilità, riguardo le sezioni dedicate alle TIC, sia la pagina web dell'Istituto.

A tale scopo, attraverso la figura dell'animatore digitale e del Referente per il cyberbullismo, l'Istituto attiverà iniziative per sensibilizzare le famiglie riguardo l'utilizzo responsabile della rete e rischi connessi.

## *Il nostro piano d'azioni*

### AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024)

**Scegliere almeno 1 di queste azioni**

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare incontri con esperti per i docenti sulle competenze digitali

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

**Scegliere almeno 1 di queste azioni**

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- 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.

Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc. La nostra scuola è impegnata in prima persona nella tutela della privacy degli utenti attraverso l'applicazione del regolamento d'Istituto e del patto di corresponsabilità. Particolare attenzione è data dalla nostra Istituzione, nei confronti degli studenti quando questi sono minorenni, in ottemperanza all'articolo 8 della Carta dei diritti fondamentali dell'Unione europea tutelato dal regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, recepito dal nostro ordinamento dal D.Lgs. 10 agosto 2018 n. 101, entrato in vigore lo scorso 19 settembre 2018.

La rapidità dell'evoluzione tecnologica, la globalizzazione, la condivisione e la raccolta di dati personali, hanno comportato nuove sfide per quanto riguarda la protezione dei dati personali.

L'Istituto per migliorare la sicurezza e la protezione dei dati vuole adottare ogni sorta di misura per rispettare le indicazioni normative contenute nel Regolamento Generale per la Protezione dei Dati Personali n. 2016/679 (GDPR), ossia la normativa europea in materia di protezione dei dati.

Il GDPR (General Data Protection Regulation) introduce come principale novità la centralità del principio di responsabilizzazione (accountability), e pone con forza l'accento sulla responsabilizzazione di titolari e responsabili dei dati, ossia l'adozione di comportamenti proattivi tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.

Oggetto e Ambito di applicazione delle misure da adottare per la protezione dei dati:

- Protezione dei diritti e delle libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali;
- Trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

Finalità perseguite dall'Istituto a sostegno della normativa vigente, ispirandosi ai seguenti principi generali:

- Il principio di necessità: tutti i trattamenti e le tecnologie impiegate tendono alla riduzione dell'utilizzo dei dati personali e identificativi;

- I dati e i relativi trattamenti sono acquisiti ed effettuati esclusivamente per le finalità istituzionali dell'Istituto;
- Tutti i trattamenti previsti eseguiti avvengono in ottemperanza alla normativa vigente;
- Il principio di correttezza e lealtà riguarda la garanzia sia della fedeltà dei dati che dell'integrità nelle modalità di raccolta, archiviazione e trasmissione;
- Sicurezza e protezione: i dati personali sono accessibili solamente al personale preposto e incaricato.

---

# *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.

La comunità scolastica, in virtù della continua trasformazione sociale, e di una società sempre più virtuale e connessa, si trova ad affrontare notevoli cambiamenti sia di tipo operativo, per quanto riguarda il decentramento informatico, sia per l'aspetto didattico orientato verso un uso protesico e intelligente della tecnologia. La connessione "always on ", pone l'accento sulle varie problematiche legate alla sicurezza della rete e la conseguente protezione dei dati che al suo interno sono custoditi.

Risorse informatiche utili per le esigenze operative del servizio dell'istituto:

- Dispositivi tecnologici (computer, devices, terminali, linee di comunicazione);
- Sistemi operativi, e/o software;
- Programmi applicativi o memorie esterne;
- Database per i quali si richiede riservatezza integrità e disponibilità.

Le infrastrutture informatiche raggiungono tutte le aule dell'istituto, queste sono dotate di PC portatili a diposizione dei docenti, sia per attività formale (compilazione del registro elettronico) che per attività didattica. I dispositivi informatici sono protetti da password e il loro utilizzo è riservato ai docenti. La connessione alla rete wi-fi, finalizzata allo scopo didattico, è riservata al personale docente, e si accede solo attraverso una password.

Politiche di sicurezza modulabile promosse dall'Istituto:

- Chiunque, dipendente o persona esterna, utilizzi risorse informatiche dell'istituto deve essere autorizzato da un responsabile;
- Le autorizzazioni devono garantire la riservatezza delle informazioni;
- L'impiego di persona esterna all'istituto per risorse informatiche deve essere individuabile (cartellino riconoscimento);
- Predisposizione di procedure tecniche organizzative per il sollecito riguardo possibili guasti o malfunzionamenti;
- Utilizzo di filtri e software che impediscano il collegamento a siti inadeguati;
- Protezione attraverso un uso consapevole delle password;
- L'istituto si impegna a fornire dispositivi sicuri e protetti;
- Per ogni dispositivo è possibile effettuare installazioni e aggiornamenti software;
- Per acquisire una maggiore competenza sull'uso delle tecnologie l'istituto promuoverà attività di formazione per il personale docente e di segreteria.

Il personale docente dell'istituto e/o personale di segreteria è autorizzato alla connessione internet tramite devices personali o forniti dall'Istituto, per attività didattiche, di servizio e/o formative.

Nello specifico:

- Internet può essere usato solo per scopi istituzionali e per quanto riguarda l'ambito professionale;
- Il fruitore è responsabile, civilmente e penalmente, per l'utilizzo del servizio internet, come regolata dalla normativa vigente;
- È vietato inserire nei devices dell'istituto programmi non autorizzati e/o scaricare o installare software non leciti (senza licenza).

Comportamenti adeguati alla professione:

- Non è opportuno utilizzare durante le lezioni, da parte dei docenti, telefoni cellulari, se non per scopi previsti istituzionalmente o per integrare le attività didattica;
- L'utilizzo dei dispositivi interattivi all'interno delle classi è subordinato alla responsabilità del docente;
- Gli studenti possono utilizzare devices all'interno della scuola in coerenza con le attività didattiche e sotto la guida e supervisione del docente;
- All'interno dell'istituto la rete internet non può essere utilizzata per scopi diversi da quelli strettamente collegati alle attività didattiche;
- L'uso di fotocamere e registratori audio/video collegato alla rete non è consentito se non autorizzato, ai sensi della normativa vigente;
- Tutti i fruitori del servizio informatico sono tenuti al rispetto delle regole di correttezza e copyright, per quanto riguarda la proprietà intellettuale, del materiale a vario titolo consultato;
- Ogni fruitore è responsabile dell'utilizzo dei dispositivi informatici a lui affidati ed utilizzati per scopi didattici e/o professionali.

---

# *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.

Per il nostro Istituto durante gli anni scolastici 2019-20 e 2020-2021 è stato fondamentale il contributo delle tecnologie digitali al fine di garantire il diritto allo studio durante il periodo dell'emergenza Covid-19. L'esperienza e le competenze

maturate da tutte le componenti della scuola somo state proficuamente impiegate e, all'occorrenza, implementate nel corso dell'a.s., 2020-21 al fine di applicare la DDI, secondo quanto previsto dal MIUR.

Pertanto, in continuità con le linee applicate negli ultimi anni nell'ambito del PNSD, pur nel rispetto della libertà di docenza dei singoli docenti, l'istituto cercherà di proseguire una didattica che integri le metodologie della didattica "tradizionale" con l'impiego consapevole delle tecnologie digitali, tramite la valorizzazione della strumentazione a disposizione. Strumenti di comunicazione fondamentali per l'utenza sono il sito istituzionale, il sistema di Meeting Cisco Webex e il Registro elettronico.

---

# *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.

"Il Piano Nazionale Scuola Digitale è un pilastro fondamentale su cui si basa "La Buona Scuola" (Legge 107/2015), una visione operativa che rispecchia la posizione del Governo rispetto alle più importanti sfide di innovazione del sistema pubblico; al centro di questa visione, vi sono l'innovazione del sistema scolastico e le opportunità dell'educazione digitale.

In questo paradigma, le tecnologie diventano abilitanti, quotidiane, ordinarie, al servizio dell'attività scolastica, in primis le attività orientate alla formazione e all'apprendimento, ma anche l'amministrazione, contaminando - e di fatto ricongiungendoli - tutti gli ambienti della scuola: classi, ambienti comuni, spazi laboratoriali, spazi individuali e spazi informali".

I danni causati per negligenza, incuria o frutto di gesti inadeguati da parte di chiunque saranno risarciti dai responsabili. Il danno causato dai minori, previa valutazione della situazione da parte dell'Istituto, sarà risarcito dai genitori.

Tutte le dotazioni e strumentazioni TIC sono fruibili solamente per scopo didattico ed è esclusivamente riservato a docenti e studenti. I docenti hanno il compito di vigilare sull'utilizzo delle infrastrutture multimediali all'interno delle aule e laboratori, ma hanno altresì il compito di formare gli alunni al rispetto delle dotazioni TIC e conseguente applicazione.

I docenti nell'esercizio della professione hanno la possibilità di utilizzare devices per scopi didattici, per integrare la didattica tradizionale o per raggiungere studenti nelle aree virtuali create ed utilizzate.

Norme di comportamento della comunità scolastica:

- È proibito utilizzare fotocamere e registratori audio/video se non autorizzato;
- Non è acconsentito modificare le impostazioni internet tali da compromettere le impostazioni di sicurezza;
- Il docente è responsabile della consultazione on line nell'ambito dell'orario di servizio all'interno della classe;
- La cura delle informazioni condivise sulle piattaforme on line è un dovere di ogni cittadino virtuale;
- Tutta la comunità scolastica è tenuta alle regole della correttezza riguardo la proprietà intellettuale (copyright);
- Tutta la comunità scolastica è responsabile dell'integrità di arredi e attrezzature informatiche di proprietà della scuola.

## *Il nostro piano d'azioni*

**AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024).**

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte deglistudenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti

**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 gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

# 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.*

Al fine della sensibilizzazione e prevenzione, il nostro Istituto si propone di educare, informare e responsabilizzare gli alunni sui rischi che corrono ogni giorno in Rete, senza demonizzarla, bensì sollecitandone un utilizzo consapevole, in modo che Internet possa rimanere per loro una fonte di divertimento e apprendimento. In questa ottica la nostra scuola intende attivare percorsi di educazione alla legalità e alla cittadinanza

digitale, oltre che promuovere le competenze previste dal curriculo digitale.

---

# *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).

Sulla base delle differenti modalità in cui avviene l'aggressione on line, sono state individuate 8 diverse categorie di cyberbullismo:

1. Flaming: messaggi online violenti e volgari indirizzati con lo scopo di suscitare vere e proprie battaglie verbali, tra due o più soggetti, all'interno di forum, chatroom e gruppi online;
2. Harassment: messaggi offensivi e molesti inviati ripetutamente alla stessa persona. In questo caso la persona che riceve gli insulti rientra a tutti gli effetti nella categoria di vittima, perché indifesa e del tutto incapace di reagire alle molestie subite;
3. Cyberstalking: ripetuti tentativi di contatto che il molestatore tenta di instaurare con la sua vittima attraverso l'utilizzo dei media digitali;
4. Denigration: diffusione, da parte del molestatore, di pettegolezzi, calunnie e offese all'interno di comunità virtuali allo scopo di danneggiare la reputazione della vittima;
5. Impersonation: vera e propria sostituzione di persona che consiste nel violare l'identità virtuale della vittima con l'obiettivo di darle una cattiva immagine e danneggiarne la reputazione
6. Trickery: pubblicazione e diffusione di informazioni riservate e/o imbarazzanti estorte alla vittima con l'inganno, dopo aver instaurato con lei un clima di fiducia al solo scopo di danneggiarla;
7. Exclusion: esclusione deliberata di una persona da un gruppo online allo scopo di suscitare in essa un sentimento di emarginazione;
8. Exposure: la pubblicazione online di informazioni private e/o imbarazzanti su un'altra persona.

Indicatori di segnali che può manifestare una potenziale vittima di cyberbullismo sono: appare nervosa quando riceve un messaggio o una notifica; sembra a disagio nell'andare a scuola o finge di essere malata (ha spesso mal di stomaco o mal di testa); cambia comportamento ed atteggiamento in modo repentino; mostra ritrosia nel dare informazioni su ciò che fa online; soprattutto dopo essere stata online, mostra rabbia o si sente depressa; inizia ad utilizzare sempre meno PC e telefono (arrivando ad evitarli); pierde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva; il suo rendimento scolastico peggiora. Finalità condivisa tra scuola e famiglia è intervenire preventivamente ed efficacemente, al fine di evitare, arginare ed eliminare possibili manifestazioni di comportamenti antisociali. Valutare i comportamenti che sfociano in disagio sociale è precursore di un lavoro in rete, con la possibilità di coinvolgere anche un servizio specialistico socio-sanitario (Psicologo della scuola, Consultorio familiare, Servizi di Neuropsichiatria, etc.), quale supporto e/o forme di mediazione.

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

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

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

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

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

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

- Condivisione nei Consigli di Classe di percorsi trasversali di Educazione civica tesi alla promozione dei diritti umani;
- Sviluppo delle competenze digitali ed educazione ad un uso etico e consapevole delle tecnologie per la promozione della consapevolezza di queste dinamiche in rete;
- Interventi finalizzati a stimolare le abilità emotive ed empatiche degli studenti;
- Percorsi di riflessione e responsabilizzazione sull'uso delle parole;
- Redazione di decaloghi condivisi dagli alunni al fine di diffondere l'uso di un linguaggio non offensivo, anche avvalendosi del supporto di materiali presenti sulla Piattaforma Generazioni Connesse.

---

# 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?*

La pervasività della tecnologia nella vita moderna, soprattutto per la generazione dei cosiddetti nativi digitali, rende indispensabile la formazione all'uso corretto delle TIC, non solo in termini di educazione ai contenuti, ma anche di educazione ai tempi di utilizzo. Talvolta infatti, la tecnologia può indurre a quella che si definisce "dipendenza da internet", ossia un progressivo e totale assorbimento del soggetto alla rete. In caso di dipendenza, l'attività on line domina il soggetto assumendo un valore primario tra tutti gli interessi e riuscendo ad influire sulle alterazioni del tono dell'umore. Una delle declinazioni della dipendenza da internet è la NOMOFOBIA, ossia l'insieme di emozioni negative quali ansia, disagio e rabbia legati alla mancanza di connessione del soggetto col proprio smartphone. Troppo spesso il tempo trascorso in rete è impiegato nelle attività di gioco virtuale che in taluni casi può creare una vera e propria dipendenza (Net Gaming Addiction o Internet Gaming Addiction). Quella da gioco in rete presenta i sintomi di una vera e propria dipendenza quali un totale assorbimento al gioco, un'ossessione nei confronti delllo stesso e il continuo impulso da parte del giocatore a giocare; impulso che, se non soddisfatto, porta a stati di agitazione, ansia o depressione. Fondamentale è dunque che la scuola formi i ragazzi affinché l'uso della rete sia sempre sereno e consapevole, in modo da favorire il benessere digitale dei ragazzi stessi. Qualora si riscontrino casi che coinvolgano gli studenti dell'Istituto in accordo con le famiglie saranno proposti eventuali percorsi educativi e/o di supporto psicologico ad opera di personale specializzato.

---

# *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 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. I contenuti sessualmente espliciti 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.

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 materiiale 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.

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. Questo fenomeno richiede più utilmente di porre l’attenzione sulla necessità della prevenzione: i più giovani devono acquisire quelle competenze in grado di orientarli e guidarli nelle loro scelte anche online; per questo motivo, come già sottolineato, l’educazione, compresa l’educazione all’affettività, riveste un ruolo fondamentale.

---

# *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.

**Da implementare con le indicazioni contenute nella lezione.**

---

# *4.7 - Pedopornografia*

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

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

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

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e

selezionando il tipo di informazioni che si possono condividere.

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

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

**Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children.**

**Da implementare con le indicazioni contenute nella lezione.**

## *Il nostro piano d'azioni*

**AZIONI (da sviluppare nell'arco dell'anno scolastico 2023/2024).**

☐ 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.

**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, 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.

# 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.

Si considerano da segnalare tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o un piccolo gruppo) tramite un utilizzo irresponsabile di internet. La scuola, quindi, avrà cura di porre attenzione alla rilevazione di rischi connessi alla navigazione sul web, in modo particolare al cyberbullismo, all'adescamento online e al sexting. In particolare dovranno essere segnalati:

- 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.

I Docenti sono tenuti a svolgere attività di rilevazione attraverso osservazioni costanti e, qualora si rendano conto di trovarsi di fronte a situazioni di criticità, dovranno rivolgersi ai Referenti, che avvieranno le procedure con le istituzioni preposte, nonché la segnalazione alla Dirigenza Scolastica. Essi avranno a disposizione uno strumento di segnalazione (vedi allegati), sul quale descrivere le situazioni che si verranno a determinare. E' opportuno che il personale della scuola, anche con l'ausilio del personale di assistenza tecnica e dell'Animatore digitale, provveda a conservare le eventuali tracce di una navigazione non consentita su Internet o del passaggio di materiali inidonei sui pc della scuola; la data e l'ora consentiranno di condurre più approfondite indagini; nel caso di messaggi, si cercherà di risalire al mittente attraverso i dati del suo profilo. Sia nel caso di chat che di messaggi di posta elettronica, l'insegnante dovrà copiare e stampare i messaggi per fornire le eventuali prove dell'indagine sugli abusi commessi. Tali prove saranno utili anche ad informare la famiglia dell'alunno vittima di abuso.

In base all'entità dei fatti si provvederà:

- a una comunicazione scritta tramite diario alle famiglie;
- a una nota disciplinare sul registro di classe;
- a una convocazione formale dei genitori degli alunni, tramite segreteria;
- a una convocazione delle famiglie da parte del Dirigente Scolastico.

Per i reati più gravi gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti). Inoltre ci si potrà avvalere dei due servizi messi a disposizione dal Safer Internet Center il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children. Una volta ricevuta la segnalazione, infatti, gli operatori procederanno a coinvolgere le autorità competenti in materia.

---

# *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.

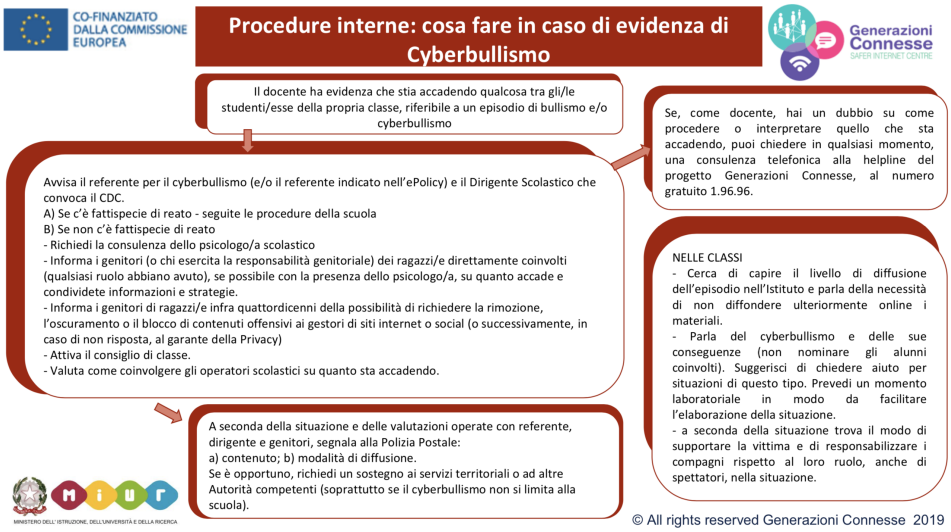
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **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.

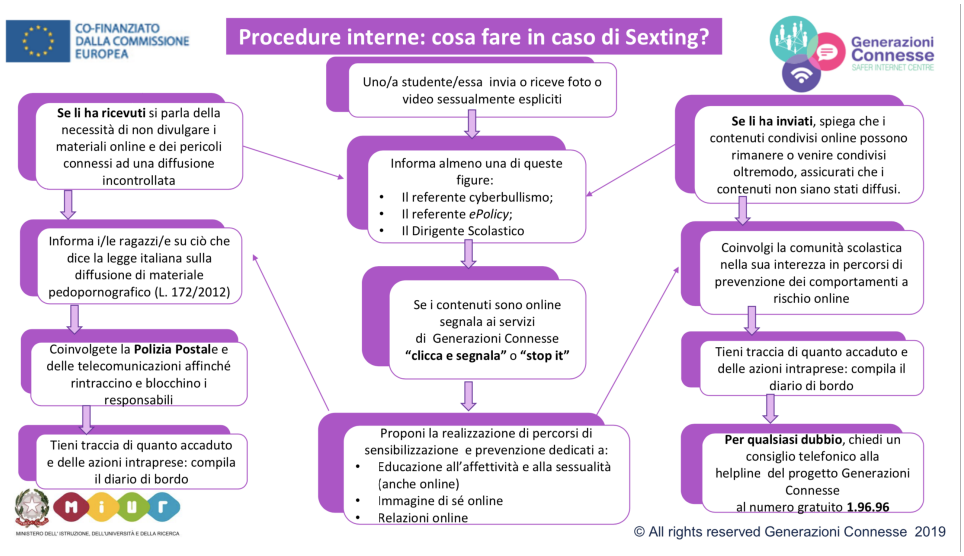
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico**: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni 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*

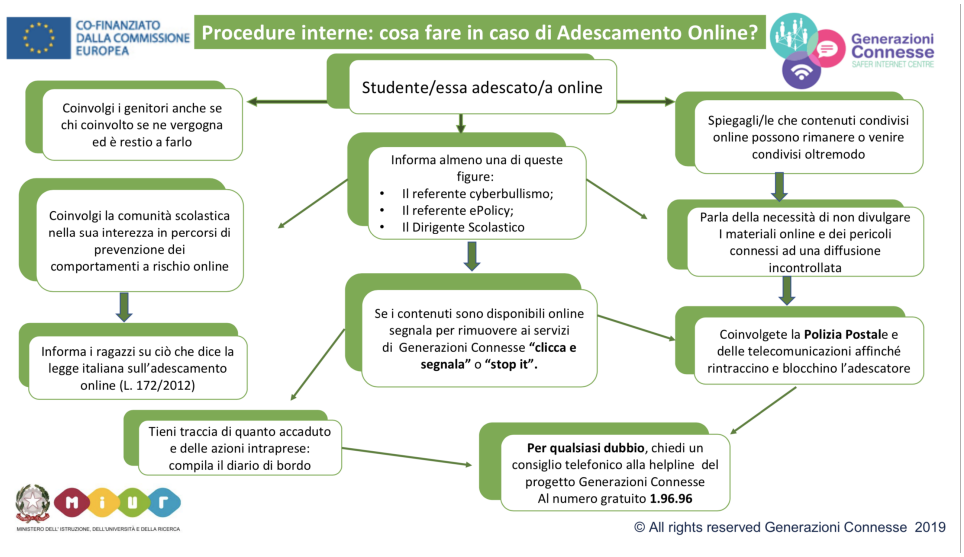
## Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



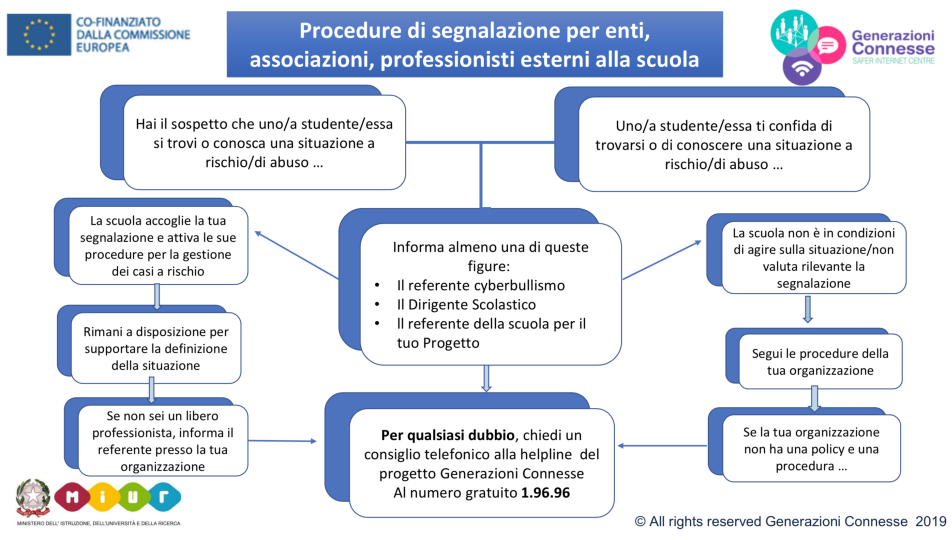

# Procedure interne: cosa fare in caso di sexting?




# 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*

Sulla base delle Linee Guida per l'uso positivo delle tecnologie digitali e della prevenzione dei rischi nelle scuole, vengono assunti i seguenti punti quali indicatori di co-costruzione tra scuola-famiglia-servizi territoriali, al fine di creare un modello composito e lineare di azioni condivise:

- coinvolgimento di tutti gli attori della scuola: studenti e studentesse, docenti, genitori e personale ATA, per la realizzazione di una autentica comunità educante; alleanza educativa tra scuola e famiglia;
- interventi educativi ed azioni di supporto, quale prevenzione per eventuali comportamenti a rischio;
- misure preventive specifiche di tutela anche con l'ausilio di attori territoriali;
- promozione dell'educazione al rispetto;

- sviluppo del pensiero critico; promozione dell'Educazione Civica Digitale.

FRANCESCO MEZZACAPO
19.05.2023 08:16:41 UTC