# Documento di ePolicy

MIIC85400Q

IC DUCA D' AOSTA -OSSONA

VIA DANTE 1 - 20010 - OSSONA - MILANO (MI)

Alessandro Lattanzi

# Capitolo 1 - Introduzione al documento di ePolicy

## *1.1 - Scopo dell'ePolicy*

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

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

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

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

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

# Argomenti del Documento


1. **Presentazione dell'ePolicy**
    1. Scopo dell'ePolicy
    2. Ruoli e responsabilità
    3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
    4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
    5. Gestione delle infrazioni alla ePolicy
    6. Integrazione dell'ePolicy con regolamenti esistenti
    7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
2. **Formazione e curricolo**
    1. Curricolo sulle competenze digitali per gli studenti
    2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
    3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
    4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
    1. Protezione dei dati personali
    2. Accesso ad Internet
    3. Strumenti di comunicazione online
    4. Strumentazione personale
4. **Rischi on line: conoscere, prevenire e rilevare**
    1. Sensibilizzazione e prevenzione
    2. Cyberbullismo: che cos'è e come prevenirlo
    3. Hate speech: che cos'è e come prevenirlo
    4. Dipendenza da Internet e gioco online
    5. Sexting
    6. Adescamento online
    7. Pedopornografia
5. **Segnalazione e gestione dei casi**
    1. Cosa segnalare
    2. Come segnalare: quali strumenti e a chi
    3. Gli attori sul territorio per intervenire
    4. Allegati con le procedure


# Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

L'Istituto Comprensivo Statale "Duca D'Aosta" ha ritenuto opportuno dotarsi di una policy di e-safety per essere pronto a cogliere i cambiamenti sociali, economici, culturali e tecnologici del contesto in cui opera, in particolare per quanto riguarda la formazione dei cittadini del futuro, destinati a vivere in un ambiente in cui tutto viene gestito attraverso l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC). Tali tecnologie diventano abilitanti, quotidiane, ordinarie, al servizio dell'attività scolastica e di tutti i suoi ambienti, coinvolgendo sia le attività orientate alla formazione e all'apprendimento sia l'amministrazione, con ricadute estese al territorio.

Con questa policy si vuole regolamentare l'uso di Internet, per rendere responsabili tutti gli utenti della scuola in modo tale da garantire la privacy all'interno dei plessi e degli uffici di segreteria. Inoltre, il curricolo pone l'accento sulle competenze digitali degli studenti, ai quali è richiesto di sapersi orientare nelle molteplici possibilità offerte da Internet, analizzando criticamente i materiali disponibili e scambiando informazioni ed esperienze in modo consapevole. Occorre in tal senso informare e formare, in particolare gli alunni, in merito a eventuali rischi e fornire misure atte a prevenirli, permettendo di beneficiare in sicurezza delle opportunità offerte da Internet e dalle TIC.

La policy di e-safety verrà revisionata e aggiornata annualmente, anche in base a eventuali variazioni delle dotazioni tecnologiche e dei protocolli dell'Istituto.

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

a) individuare un insieme di regole, di comportamenti e descrive le misure di prevenzione, per la rilevazione e gestione delle problematiche legate ad un utilizzo scorretto degli strumenti digitali;

b) promuovere l'educazione alle tematiche connesse alle "competenze digitali": uso consapevole della rete; internet, privacy, sicurezza online e uso delle tecnologie digitali nella didattica e nel percorso educativo;

c) sensibilizzare e prevenire i fenomeni legati ai rischi delle tecnologie digitali;

d) rilevare, segnalare i casi individuati all'interno della scuola legati al fenomeno del bullismo e/o all' uso non corretto delle tecnologie digitali;

e) gestire i casi, ovvero le misure che la scuola intende attivare a supporto delle famiglie e degli studenti che sono stati vittime o spettatori attivi e/o passivi di quanto avvenuto.

---

# *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 Dirigente Scolastico

Il Dirigente Scolastico deve garantire la sicurezza, anche online, di tutti i membri della comunità scolastica. Sarebbe importante, quindi, che fosse 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; potrebbe, inoltre, promuovere la cultura della sicurezza online e, ove possibile, dare il proprio contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC. Il Dirigente Scolastico ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

**L'Animatore digitale**

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

**Il Referente bullismo e cyberbullismo**

"Ogni Istituto scolastico, nell'ambito della propria autonomia, individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo" (Art. 4 Legge n.71/2017, "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo" (permalink – file 1 LEGGE 71_2017 in allegato). Tale figura ha il compito di coordinare e promuovere iniziative

specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Fondamentale, dunque, il suo ruolo non solo in ambito scolastico ma anche in quello extrascolastico, in quanto (ove possibile) potrebbe coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori (un approfondimento maggiore sui ruoli relativi alle problematiche del bullismo e del cyberbullismo verrà fornito nel modulo 4, al paragrafo 4.2.).

**I Docenti**

I Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Potrebbero, innanzitutto, integrare parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica. I docenti dovrebbero 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)**

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

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

**I Genitori**

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

**Gli Enti educativi esterni e le associazioni**

gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola dovrebbero conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC; dovrebbero, inoltre, promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme. A tal fine suggeriamo di prevedere una sezione specifica dell'ePolicy con indicazioni ad hoc e procedure standard per gli attori esterni.

---

# *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).

**Ambiti di applicazione, attività e ruoli**

Le attività progettuali o di formazione a carattere seminariale, devono essere preventivamente autorizzate dal Dirigente scolastico, con modalità e tempi concordati; a tal proposito, al fine di verificare preventivamente il contenuto da somministrare o dibattere con la scolaresca, i soggetti esterni forniranno un dettagliato programma delle attività con narrazione sintetica della scaletta al fine di essere autorizzato dalla Dirigenza.

---

# *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.

**Condivisione e comunicazione della e-policy agli studenti e alle studentesse**

- All'inizio dell'anno, in occasione dell'illustrazione del Regolamento di Istituto agli alunni da parte dei docenti, verrà presentata la e-policy insieme ai regolamenti correlati e al patto di corresponsabilità.

- Tutti gli alunni saranno informati che la rete, l'uso di internet e di ogni dispositivo digitale saranno controllati dai docenti e utilizzati solo con la loro autorizzazione e

supervisione.

- L'elenco delle regole per la sicurezza on-line sarà pubblicato in tutte le aule o laboratori con accesso a internet.

- Sarà data particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili, con specifico riferimento al contrasto di ogni forma di cyberbullismo.

**Condivisione e comunicazione della epolicy al personale scolastico**

- Le norme adottate dalla scuola in materia di sicurezza dell'uso del digitale saranno discusse dagli organi collegiali e rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito istituzionale.

- Il personale scolastico riceverà un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso materiali resi disponibili anche sul sito istituzionale nonchè mediante la partecipazione a incontri formativi organizzati dall'Istituto.

- Tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

**Condivisione e comunicazione della epolicy ai genitori**

- Sarà favorito un approccio collaborativo nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione di incontri scuola- famiglia assembleari, collegiali e individuali al fine di sensibilizzare le famiglie sui temi dell'uso delle TIC.

- Saranno organizzati incontri informativi per presentare e condividere la presente e-policy.

- E' fondamentale condividere e comunicare il documento ai genitori sul sito istituzionale della scuola, nonché tramite momenti di formazione specifici e durante gli incontri scuola-famiglia.

La ePolicy, dopo essere stata approvata dal collegio Docenti e dal Consiglio di Istituto, sarà inserita all'interno del PTOF.

---

# *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.

Nel caso in cui una violazione al regolamento di istituto si configuri come atto di bullismo\cyberbullismo, colui che ne viene a conoscenza informa tempestivamente il Dirigente Scolastico e il referente per il bullismo/cyberbullismo. Qualora tali infrazioni dovessero configurarsi come reato, il Dirigente Scolastico farà una tempestiva segnalazione all'autorità competente fatto obbligo di denuncia (ex art. 331 del Codice di Procedura Penale). Si rinvia al Regolamento d'Istituto, al Regolamento di Disciplina e al Patto di Corresponsabilità.

**Disciplina 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;

- Invio di immagini o video volti all'esclusione di compagni/e;

- Comunicazione incauta e senza permesso con sconosciuti;

- Collegamenti a siti web non adeguati e non indicati dai docenti.

L'azione educativa prevista per gli alunni è 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 di alcune attività);

- 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 rispetto a comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle 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.

**Disciplina 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 rischi connessi;

- Insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.

Il Dirigente scolastico può disporre il controllo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola; può disporre la cancellazione di materiali non adeguati o non autorizzati dal sistema informatico della scuola, e se necessario ne conserva una copia per eventuali approfondimenti successivi.

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 dei procedimenti che possono avere carattere organizzativo-gestionale, disciplinare, amministrativo, penale, a seconda del tipo e della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

**Disciplina dei genitori**

In considerazione dell'età degli studenti e delle studentesse e della loro dipendenza dagli adulti, anche talune condizioni e condotte dei genitori medesimi possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli allievi a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico. Gli atteggiamenti da parte della famiglia meno favorevoli sono:

- La convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non corre rischi;

- Una posizione del computer in una stanza o in una posizione non visibile e controllabile dall'adulto;

- Una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'uso di cellulare o smartphone;

- Un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei a minori;

- Un utilizzo di cellulari e smartphone in comune con gli adulti che possono conservare in memoria indirizzi di siti o contenuti non idonei a minori;

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 sè e/o dannosi per altri (culpa in educando e in vigilando).

---

# *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 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 Policy e del suo eventuale aggiornamento sarà curato dal Dirigente Scolastico con la collaborazione dell'Animatore digitale, del Team digitale, del referente del bullismo e cyberbullismo e del relativo gruppo di lavoro.

Avrà il fine di rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di Internet.

Il monitoraggio on-line sarà rivolto anche ai docenti, al fine di valutare l'impatto della Policy e la necessità di eventuali miglioramenti. L'aggiornamento della Policy sarà curato dal Dirigente scolastico, dall'Animatore digitale, dal Team, dal responsabile del bullismo e cyberbullismo, dalla commissione bullismo e dagli Organi Collegiali.

---

# *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 Policy avverrà:

- All'inizio di ogni anno scolastico, contestualmente alla revisione del PTOF, a cura del Dirigente scolastico, dell'Animatore digitale, con il gruppo di lavoro, e dei collaboratori del Dirigente;

- A seguito di verifica atta a constatare l'insorgenza di nuove necessità e la revisione di tecnologie esistenti;

- Alla fine di ogni anno scolastico, contestualmente al Rapporto di Autovalutazione e sulla base dei casi problematici riscontrati e della loro gestione.

---

## *Il nostro piano d'azioni*

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

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

**Azioni da svolgere nei prossimi 3 anni:**

- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare un evento di presentazione del progetto Generazioni Connesse 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.

L'Istituto, come evidenziato nel Piano Triennale dell'Offerta Formativa, pone particolare attenzione allo sviluppo della competenza digitale dei propri studenti, in linea con quanto previsto dal Piano Nazionale per la Scuola Digitale (PNSD). Questa competenza non può essere sciolta dalle competenze sociali e civiche che ogni alunno deve maturare, soprattutto per gli aspetti relazionali da esse implicati: l'ascolto, il rispetto reciproco, la capacità di vivere insieme. In tal modo ci si prefigge di prevenire eventuali fenomeni di disagio giovanile (bullismo, cyberbullismo, violenza, discriminazioni, uso di sostanze stupefacenti…). La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni, nonché per comunicare e partecipare a reti collaborative tramite Internet. Si pone quindi enfasi sulla capacità di esplorare e affrontare in modo flessibile situazioni tecnologicamente nuove,

adeguando le performance ai diversi contesti in cui si opera, in modo tale da:

- Analizzare e valutare criticamente i dati e le informazioni con cui ci si confronta durante la navigazione online e l'uso delle TIC;

- Sfruttare le potenzialità offerte dalle TIC per la risoluzione di problemi;

- Costruire e condividere le conoscenze acquisite, sviluppando una consapevole responsabilità in merito ai dati personali e alla tutela della privacy, con particolare attenzione ai diritti e doveri reciproci degli utenti. La competenza digitale è data dalla fusione delle dimensioni: etica, inerente alla responsabilità sociale, al sapere relazionarsi con gli altri utenti, al tenere dei comportamenti adeguati alle circostanze in cui ci si può imbattere e alla tutela della propria persona, per preservare la quale è necessario sapersi schermare dai possibili rischi; tecnologica, il saper individuare gli usi e i punti di forza dei dispositivi in uso e, quindi, scegliere i device e i mezzi adeguati per risolvere problemi; cognitiva, grazie alla quale è possibile saper leggere, selezionare e valutare dati, attraverso modelli astratti che conducano a un'analisi critica degli stessi al fine di individuare le informazioni attendibili e pertinenti al compito affidato tra tutte quelle offerte dalla Rete.

Per perseguire questi traguardi, i docenti adottano, come supporto alle attività scolastiche, le tecnologie educative e didattiche a disposizione, quali LIM, libri di testo digitali, risorse multimediali. Grazie a una didattica mediale in cui i media sono visti come un supporto fondamentale per un apprendimento disciplinare efficace, ai docenti spetta il compito di promuovere una riflessione critica e una sperimentazione creativa, approfondendo le dinamiche che regolano il sistema dei media stessi, la decodifica dei messaggi e la conoscenza dei linguaggi mediali. Ciò è realizzabile grazie a un approccio costruttivista, basato sull'apprendimento, e a metodi di insegnamento quali flipped classroom, EAS e via discorrendo. L'Istituto, coerentemente con quanto previsto dal PNSD, attiva dei percorsi di formazione rivolti ai docenti per acquisire le competenze necessarie.

---

# *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.

L'Istituto, ancor prima del sorgere dell'emergenza sanitaria, causata dalla pandemia Covid-19, aveva due figure di riferimento per quanto riguarda l'uso, l'implementazione nella didattica e la manutenzione delle nuove tecnologie, vale a dire l'animatore digitale e una funzione strumentale.

Le due figure, in stretta collaborazione, hanno sempre proposto e favorito la formazione dei docenti dell'Istituto, nei tre ordini di scuola, riguardo l'uso e integrazione delle TIC nella didattica, sia per quanto riguarda la gestione dei dispositivi (LIM, monitor touch, notebook, tablet), che per la parte software (browser, internet security, programmi di scrittura, fogli di calcolo, creazione di presentazioni, registro elettronico, lavagne multimediali, piattaforme per il coding).

Durante la pandemia (anni scolastici 2020-21 e 2021-22), le esigenze della didattica a distanza hanno riconfigurato le priorità riguardanti la formazione dei docenti, spostando l'asse verso l'uso delle app di Google per la gestione delle classi virtuali, lezioni sincrone, comunicazione con colleghi, dirigenza, studenti, amministrazione e famiglie (GSuite for Education).

Attualmente, l'Istituto, attraverso la figura dell'animatore digitale, propone corsi di formazione, soprattutto in modalità online (asincrona e sincrona), sull'implementazione degli strumenti, usati durante la didattica a distanza, in quella in presenza, con il fine di adoperare una vera e propria didattica digitale integrata, ormai necessaria nella vita quotidiana e lavorativa del ventunesimo secolo.

Inoltre, una parte dei docenti, è formata sull'utilizzo di strumenti per condurre attività didattiche di coding e robotica educativa nei tre ordini di scuola presenti nell'istituto.

---

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

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

personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc…), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

L'Istituto, a partire dall'anno scolastico 2020/21, si è dotato di un gruppo di lavoro per la stesura del documento di ePolicy, formato dall'animatore digitale, il team di innovazione e quello di prevenzione al bullismo e cyberbullismo, i cui docenti provengono dai tre ordini di scuola dell'Istituto, affinché si collabori e si agisca in verticale, a partire dalla scuola dell'infanzia.

Il gruppo di lavoro si è formato grazie ai corsi proposti dalla piattaforma di "Generazioni Connesse" e, dopo aver condiviso il documento con l'intera comunità scolastica, proporrà iniziative di formazione sul'utlizzo consapevole di internet e delle tecnologie digitali, sia per poter, a loro volta, indirizzare gli studenti in tal senso, sia per poter prevenire fenomeni di bullismo e cyberbullismo.

In parallelo, il personale dell'Istituto, docente e non, ha seguito un corso online sulla privacy nel mondo della scuola e la gestione dei dati sensibili propri e degli utenti (famiglie e studenti).

---

# *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.

All'interno del Patto di Corresponsabilità condiviso dall'Istituto con le famiglie e gli studenti, è già presente una sezione dedicata all'uso consapevole delle TIC, nella quale è stabilito cosa si impegnano a fare i tre attori principali della comunità scolastica: è

riportato che la scuola si impegna a "A tutelare la sicurezza degli alunni nell'uso delle TIC, educandoli ad un uso corretto dei dispositivi multimediali e della Rete, visionando preventivamente i siti da proporre e vigilando attentamente su tutte le operazioni svolte a scuola". Invece, gli alunni si impegnano a "attenersi scrupolosamente alle indicazioni fornite dai docenti sull'uso della Rete e dei dispositivi multimediali, utilizzando la strumentazione della scuola ed i dispositivi personali autorizzati (BYOD) solo per scopi didattici e non personali". Infine, è previsto che i genitori si impegnino a "controllare con regolarità il registro elettronico ed il sito istituzionale della scuola e a guidare i figli verso un uso responsabile e sicuro della tecnologia". L'Istituto, inoltre, ha messo a disposizione, durante l'anno scolastico 2020-21, un corso di formazione sulla gestione della GSuite For Education per le famiglie.

Oltre a quanto riportato nel Patto, il Regolamento d'Istituto, aggiornato al mese di gennaio del 2021, prevede una sezione riguardante l'uso delle nuove tecnologie, nella quale sono contenuti chiarimenti e norme su utilizzo di quest'ultime e di internet a scuola, gestione del sito web dell'Istituto, uso dei laboratori di informatica, utilizzo dei telefoni cellulari e dei dispositivi elettronici e, infine, riporta anche le norme della "Netiquette".

Infine, dopo le prime fasi della didattica a distanza, è risultato necessario elaborare anche il Regolamento per la Didattica Digitale Integrata, approvato nel mese di settembre 2020 Quest'ultimo stabilisce le modalità di attuazione di questa tipologia di didattica e della partecipazione nella stessa di tutte le componenti della Scuola.

I suddetti documenti, verranno aggiornati a seguito dell'approvazione del documento di ePolicy, prevedendo l'organizzazione di percorsi di sensibilizzazione e formazione dei genitori su un uso responsabile e costruttivo della Rete in famiglia e a scuola. Un ulteriore obiettivo è il coinvolgimento delle famiglie in tali percorsi di sensibilizzazione, mediante l'organizzazione di iniziative in cui anche gli studenti e le studentesse siano protagonisti.

## *Il nostro piano d'azioni*

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

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

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

- 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.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

## *3.1 - Protezione dei dati personali*

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

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

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

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

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

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

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

**Art. 37 Regolamento istituto:**

**Dati personali – privacy**

I dati personali che vengono raccolti, registrati, elaborati, conservati, diffusi vengono trattati - per obbligo di legge - per regolamento interno - per deliberazione del Consiglio di Istituto 19 esclusivamente per le finalità istituzionali della scuola. I dati personali vengono resi pubblici nei casi previsti da leggi o regolamenti (es. pubblicazione dei risultati finali dell'anno scolastico oppure degli organici del personale) e non vengono comunicati ad associazioni o enti se ciò non è indispensabile per le attività previste quali visite didattiche, assicurazioni volontarie, partecipazione a concorsi ecc.. Questionari o sondaggi, raccolte di dati informativi possono essere effettuati soltanto in forma anonima; eventuali modalità diverse devono essere espressamente autorizzate dal Consiglio di Istituto. All'atto della prima iscrizione i genitori degli alunni possono non autorizzare le fotografie e le videoriprese.

---

# *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.

**Da regolamento di istituto**:

Il curricolo scolastico prevede che gli alunni imparino ad utilizzare le TIC (Tecnologie di Comunicazione Informatica) e la ricchezza della rete internet in funzione dell’apprendimento. L’utilizzo delle nuove tecnologie consente inoltre di formare gli alunni su importanti temi di cittadinanza, quali la pluralità delle fonti di informazione, il diritto d’autore e i rischi della rete.

Gli insegnanti hanno la responsabilità di guidare gli alunni nelle attività on line, di stabilire obiettivi chiari nell'uso di Internet e insegnarne un uso accettabile e responsabile. L'obiettivo principale resta quello di arricchire ed ampliare le attività didattiche, secondo quanto prevede il curricolo scolastico, l’età e la maturità degli alunni.

**Utilizzo di internet**

L’accesso ad internet è libero per il personale in servizio presso l’Istituto nell’ambito della propria attività professionale. Qualsiasi utilizzo improprio o che esuli dalle esigenze scolastiche ricadrà sotto l’esclusiva responsabilità personale. La connessione a Internet da parte degli alunni, invece, può avvenire solo previa autorizzazione del docente e sempre sotto il vigile controllo del docente stesso che deve essere presente in laboratorio. Non è opportuno che gli alunni utilizzino a scuola la posta elettronica personale. Per tutti gli utenti, accedendo a Internet, occorre rispettare la “netiquette” (regole di comportamento) esplicitata nel presente Regolamento. È fatto divieto di accedere a siti non legati ad attività didattiche e di utilizzare internet per scopi vietati dalla legislazione vigente. Si ricorda che l'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi per l'uso fatto del servizio

Internet. E' vietato inoltre scaricare da Internet software non autorizzati e installarli senza licenza.

**Tutela della privacy**

Tutto il personale è tenuto a tutelare la propria privacy e quella degli alunni: si raccomanda l'utilizzo di password qualora vengano conservati nei computer documenti strettamente personali, riferiti soprattutto ai profili dei singoli alunni o a documenti di rilevante importanza.

Ogni utente è tenuto al rispetto dell'altrui privacy e non divulgherà notizie private contenute nelle documentazioni elettroniche.

Gli indirizzi di posta elettronica degli alunni, dei genitori, dei docenti e del personale della scuola non vanno divulgati; in nessun caso l'Istituto attiverà account di posta elettronica individuali per i minori.

**Netiquette**

Fra gli utenti dei servizi telematici di rete si è sviluppata, nel corso del tempo, una serie di tradizioni e di norme di buon senso che costituiscono la “Netiquette” che si potrebbe tradurre in “Galateo (Etiquette) della Rete (Net)”.

L'elenco delle regole fondamentali che tutti gli utenti sono tenuti a seguire è affisso nei laboratori di informatica dell’Istituto.

- Non essere offensivo:

Il testo è l'unico mezzo attraverso il quale comunicare con gli altri in rete. Il tono della voce, l'espressione del viso non possono essere di aiuto per far comprendere all'altro il senso del discorso. Il rischio di essere fraintesi è altissimo. Bisogna tenerlo sempre presente quando si scrive e, se necessario, usare gli emoticons (emotional icons) per ribadire il tono del messaggio.

- Seguire regole di comportamento analoghe alle proprie regole di vita:

Utilizzare in maniera fraudolenta un prodotto a pagamento equivale ad un furto. Solo acquistandolo regolarmente s'incoraggiano i realizzatori a creare altri prodotti.

- Scegliere l’ambiente adatto a se stessi:

Ogni chat, mailing list, newsgroup, forum, blog ha delle caratteristiche specifiche. E’ importante imparare a scegliere la community che più si avvicina alle proprie esigenze, ma soprattutto quella dove ci si sente più a proprio agio, anche grazie al controllo del moderatore.

- Scegliere di essere paziente e comprensivo:

Quando si invia un messaggio non bisogna pretendere risposta. Chi comunica con noi

può non essere interessato all'argomento che proponiamo oppure può non avere il tempo di rispondere.

- Scegliere toni moderati:

Se si esprime il parere in maniera pacata è meno probabile che le parole usate possano provocare reazioni dure da chi comunica con noi. Basta poco per infiammare una discussione e serve invece molto tempo per tornare ad un dialogo tranquillo.

- Rispettare la privacy:

Usare in rete le stesse regole che si usano nella vita. Ognuno di noi ha il diritto di scegliere se condividere o meno le informazioni che lo riguardano.

- Non abusare delle proprie conoscenze:

Non usare mai le proprie competenze per entrare nel mondo altrui.

- Trascurare gli errori degli altri:

Il desiderio di rispondere velocemente porta a errori di digitazione, di grammatica o di sintassi, ma l'importante è che il messaggio sia comprensibile.

- Dimenticare le differenze:

La rete è un mondo nel quale l'unico strumento è la tastiera e l'unico oggetto visibile il monitor. Non hanno nessuna importanza il colore della pelle, la religione, ecc...

- Presentarsi con cura:

In rete si hanno solo le parole per farsi conoscere. Bisogna usarle con cura, scegliendo quelle di cui si è veramente convinti.

- Utilizzare la rete per ampliare le proprie conoscenze:

Internet è una sterminata enciclopedia a portata di mouse, ed offre anche la possibilità di leggere le opinioni degli altri su qualsiasi argomento. Si possono trovare informazioni specialistiche, materiale per ricerche scolastiche, ma potrebbe essere un valido ausilio anche solo per effettuare confronti tra le varie opinioni presenti.

- Essere prudente:

Non dare in modo affrettato informazioni personali o che riguardano la propria famiglia. Non accettare, senza riflettere, di incontrare qualcuno che si è appena conosciuto nella rete. Non credere a tutto quello che viene detto.

- Non urlare:

Scrivere in maiuscolo su Internet equivale ad urlare: è uno strumento a disposizione per enfatizzare le cose che si stanno dicendo. Attenzione a non abusarne.

# 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.

STRUMENTI DI COMUNICAZIONE ESTERNA

**Sito Web Istituzionale**

L'Istituto è dotato di un sito web raggiungibile all'indirizzo https://www.icossona.edu.it/ costantemente aggiornato da docenti esperti sotto la supervisione del DS, che ne valuta la sicurezza e l'adeguatezza sotto il profilo dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy.

Esso offre al proprio interno vari servizi tra i quali:

- piano dell'offerta formativa;

- regolamento d'Istituto;

- elenchi libri di testo;

- informazioni generali sull'Istituto;

- informazioni sull'amministrazione dell'Istituto;

- collegamento al portale del registro elettronico;

- informazioni sui progetti attivati dall'Istituto;

- avvisi e comunicazioni;

- moduli vari.

Il sito è dotato di un'area riservata, accessibile tramite credenziali personali, dove vengono pubblicate comunicazioni e modulistica riservata.

STRUMENTI DI COMUNICAZIONE INTERNA

**Registro elettronico**

Il Registro Elettronico adottato dall'Istituto è "Axios" che consente la gestione delle attività didattiche come assenze, voti, giudizi, argomenti delle lezioni, comunicazioni con le famiglie, gestione dei colloqui e annotazioni varie. L'accesso al RE è riservata e ogni famiglia riceve le credenziali per la consultazione.

**E-mail**

Tutto il personale scolastico e tutti gli alunni sono in possesso di un account istituzionale di posta elettronica con dominio icossona.edu.it

**Piattaforma "Google Suite for Education"**

La Google Suite for Education (o GSuite), in dotazione all'Istituto, è associata al dominio della scuola e comprende un insieme di applicazioni sviluppate direttamente da Google, quali Gmail, Drive, Calendar, Documenti, Fogli, Presentazioni, Moduli, Hangouts Meet, Classroom, o sviluppate da terzi e integrabili nell'ambiente, alcune delle quali particolarmente utili in ambito didattico.

I genitori degli alunni sottoscrivono l'informativa ex art. 13 del regolamento ue 2016/679, per il trattamento dei dati personali ai fini dell'iscrizione ed utilizzo della piattaforma "Google Suite for Education".

---

# *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.

Le disposizioni in materia di utilizzo di dispositivi personali a scuola hanno una valenza

educativa e formativa in quanto:

- l'utilizzo del telefono cellulare e/o di altri dispositivi elettronici rappresenta un elemento di distrazione sia per chi lo usa sia per i compagni, oltre che una grave mancanza di rispetto nei confronti del docente;

- i moderni strumenti di comunicazione si rivelano utili in moltissime occasioni, ma non possono prendere il posto delle relazioni umane che è compito della scuola valorizzare.

Agli alunni è permesso portare a scuola i telefoni cellulari, quanto ritenuto indispensabile. Come da art.20 comma 12, durante le lezioni e l'orario scolastico dovranno rimanere spenti e nello zaino. È quindi vietato ricevere/effettuare chiamate, inviare messaggi, collegarsi ad internet, effettuare registrazioni audio/video e fotografie all'interno dei locali scolastici. Il divieto non si applica soltanto all'orario delle lezioni, ma è vigente anche negli intervalli e nelle altre pause dell'attività didattica.

Il Consiglio di classe può derogare temporaneamente a tale disposizioni, consentendo di portare il cellulare, in caso di particolari situazioni non risolvibili in altro modo, su richiesta dei genitori, da inoltrare per iscritto.

Per quanto riguarda uscite, visite guidate e viaggi di istruzione, l'uso è consentito al di fuori dei momenti dedicati a visite e attività legate all'aspetto didattico dell'uscita.

Il divieto di utilizzare il cellulare ed altri eventuali dispositivi elettronici per usi che non siano strettamente didattici è da intendersi rivolto anche al personale della scuola (docenti e personale ATA) in orario di servizio.

## *Il nostro piano d'azioni*

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

-Organizzare un evento o attività volte a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola;

-Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali;

-Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali;

- Organizzare uno o più eventi o attività volti a formare 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;

- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali;

-Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity).

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

## *4.1 - Sensibilizzazione e Prevenzione*

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

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

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

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

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

L'Istituto si prefigge come obiettivo quello di fornire a tutta l'utenza le competenze necessarie al fine di tenere comportamenti responsabili e corretti nella fruizione delle TIC e della Rete, così da poter prevenire i rischi in cui ci si può imbattere.

Per quanto riguarda l'uso delle TIC, il personale in servizio presso la scuola, gli alunni e le loro famiglie sono informati e formati in merito alle modalità per utilizzare in modo sicuro, negli ambienti scolastici o all'esterno, i diversi device, quali tablet, pc, smartphone, fornendo loro indicazioni su come gestire impostazioni di cronologia, cookie, cache, firewall, malware e virus in genere.

Fondamentale è anche diffondere le nozioni per una navigazione sicura, corretta e responsabile in merito a uso di siti e piattaforme istituzionali, compresi il sito della scuola, il registro elettronico e le piattaforme usate durante le attività didattiche; gestione degli account, con attenzione alla conservazione delle credenziali di accesso; misure di sicurezza per la fornitura dei dati personali, ponendo attenzione alle situazioni in cui ciò è sconsigliato o poco opportuno; gestione e netiquette delle caselle di posta elettronica in genere e delle mailing list, anche per ciò che riguarda la possibilità di imbattersi in comunicazioni fraudolente; regole per l'upload e il download in sicurezza di qualsiasi tipo di file; gestione delle relazioni sui social network, nelle chat e nelle applicazioni di instant messaging, soprattutto a proposito della condivisione e pubblicazione di foto, video, informazioni personali, conversazioni; rischi di entrare in siti non opportuni, pornografici, di reclutamento a fini illegali, fraudolenti; rischi più diffusi in Rete, anche a causa di un utilizzo non responsabile della stessa, in particolare cyberbullismo, sexting, grooming; normativa vigente sulla privacy e sulle procedure di dematerializzazione messe in atto dalla scuola.

---

# *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).

Tutte le componenti scolastiche, in particolare personale docente e genitori, devono essere costantemente formate, informate e aggiornate sui fenomeni del bullismo e del cyberbullismo.

A tal fine, l'Istituto applica le seguenti strategie:

- interventi con associazione MOIGE, polizia postale, Pepita Onlus;

-formazione mediante l'applicazione ONE SAFE, distribuita a tutte le classi prime (genitori e docenti) e a tutti i coordinatori della secondaria di primo grado.

Si è in contatto, inoltre, con una rete di supporto territoriale, formata da diversi enti: Kinesis, il Comune attraverso l'Ufficio Servizi Sociali e altri centri di Associazioni, nonché gli organismi Istituzionali preposti.

L'Istituto si impegna a formare e aggiornare i docenti sulle modalità e gli indicatori per riconoscere eventuali casi o situazioni a rischio e sulle procedure da seguire. Chiunque entri in possesso di dati certi deve avere la possibilità di denunciarli in forma tutelata: il denunciante non deve correre rischi e deve avere tutte le possibili tutele.

Nel momento in cui si è a conoscenza di situazioni di bullismo o cyberbullismo il docente avvisa immediatamente il referente del bullismo e cyberbullismo del plesso e la dirigenza scolastica; il docente stende un verbale dell'episodio, nel quale vengono riportate le situazioni problematiche rilevate; il dirigente scolastico convoca la famiglia per informarla dell'accaduto; il docente svolge un colloquio approfondito, in separata sede, sia con la vittima sia con il bullo o cyberbullo, per acquisire informazioni

aggiuntive che è tenuto a verbalizzare; a seconda dei casi, si informano i servizi sociali e/o la Polizia Postale; in caso di eventi particolarmente gravi o con profili che si possono presumere penali, è obbligatorio ricorrere all'autorità giudiziaria; gli studenti protagonisti di atti di bullismo o cyberbullismo devono essere guidati a comprendere la gravità degli atti compiuti; devono essere sanzionati come da regolamento e, contestualmente, devono essere obbligati a comportamenti attivi di natura risarcitoria e riparatoria, volti al perseguimento di una finalità educativa (cfr. Circolare 15/05/2007, MPI); a livello formativo, i docenti tengono conto dell'accaduto nel corso del processo didattico.

Si ricorda che, in caso di necessità, ci si può rivolgere ai seguenti servizi, gestiti da Telefono Azzurro (http://www.azzurro.it/it/sostegno), come suggerito dalla Helpline di Generazioni Connesse (http://www.generazioniconnesse.it/index.php?s=38):

Linea di ascolto 1.96.96, attiva 24 ore su 24, 365 giorni all'anno; Chat, attiva dalle 8:00 alle 22:00 in settimana, dalle 8:00 alle 20:00 il sabato e la domenica.

Tali canali accolgono qualsiasi richiesta d'ascolto e di aiuto da parte di bambini e ragazzi fino ai 18 anni o da parte di adulti che si vogliono confrontare su situazioni di disagio/pericolo che vedono coinvolti dei minori, uso sicuro di Internet e dei social network, adescamento, online/grooming, pedopornografia, cyberbullismo, sexting, pornografia e sessualità online degli adolescenti, gioco d'azzardo online violazione della Privacy ,furto di identità in Rete, esposizione a contenuti nocivi online, dipendenza da Internet, esposizione a siti violenti, razzisti, che invitano al suicidio o a comportamenti alimentari scorretti (pro-anoressia e (pro-bulimia), dipendenza da shopping online, videogiochi online non adatti ai ragazzi.

Il servizio di Helpline è riservato, gratuito e sicuro, dedicato ai ragazzi e alle famiglie, che possono trovarvi un consulto con professionisti qualificati relativamente a dubbi, domande o problemi legati all'uso delle nuove tecnologie digitali e alla sicurezza in Rete.

È possibile, inoltre, usufruire del servizio Hotline, reperibile all'indirizzo http://www.generazioniconnesse.it/index.php?s=37, che raccoglie e dà corso a segnalazioni, inoltrate anche in forma anonima, riguardanti contenuti pedopornografici, illegali o dannosi presenti online. I servizi messi a disposizione dal Safer Internet Center sono Clicca e segnala, di Telefono Azzurro Stop-it, di Save the Children.

Dopo che sarà stata ricevuta una segnalazione, gli operatori provvederanno a coinvolgere, al bisogno, le autorità competenti.

Per segnalare contenuti inopportuni visionati sui media si può far riferimento al sito del CoReCom(Comitato Regionale per le Comunicazioni) all'indirizzo http://www.corecomlombardia.it/opencms/index.html.

Anche la Polizia Postale e delle Comunicazioni https://www.commissariatodips.it/ è

attualmente impegnata in attività a sostegno della navigazione protetta dei minori ed è competente a ricevere segnalazioni in merito a qualsiasi tipo di reato informatico.

---

# *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.

**Come riconoscerlo e prevenirlo**

Scopriamo insieme le caratteristiche dell'hate speech, come riconoscerlo e prevenirlo:

- Il discorso d'odio procura sofferenza.

La parola ferisce, e a maggior ragione l'odio! Il discorso può violare i diritti umani. Il discorso d'odio online non è meno grave della sua espressione offline, ma è più difficile da individuare e da combattere.

- Gli atteggiamenti alimentano gli atti.

Il discorso dell'odio è pericoloso anche perché può condurre a più gravi violazioni dei diritti umani, e perfino alla violenza fisica. Può contribuire a inasprire le tensioni razziali e altre forme di discriminazione e di violenza.

- L’odio online non è solo espresso a parole.

Internet ci permette di comunicare rapidamente e in modi svariati, ad esempio, mediante i social media e i giochi online, molto spesso, d’altronde, in maniera anonima. L’odio online può esprimersi sotto forma di video e foto, come pure, più solitamente, di contenuto testuale. Le forme visive o multimediali hanno sovente un impatto più forte sugli atteggiamenti (consci e inconsci).

- L’odio prende di mira sia gli individui che i gruppi.

L’odio online può prendere di mira dei gruppi che spesso sono già vulnerabili sotto altri aspetti, come i richiedenti asilo, le minoranze religiose o le persone con disabilità. Tuttavia, anche i singoli individui sono sempre maggiormente oggetto di attacchi. Le conseguenze sono talvolta fatali, come dimostrato da numerosi fatti di cronaca riferiti dai media, riguardanti giovani vittime di cyberbullismo che sono state spinte al suicidio.

- Internet è difficilmente controllabile.

La diffusione di messaggi di incitamento all’odio è maggiormente tollerata su Internet rispetto al mondo offline ed è sottoposta a minori controlli. È ugualmente più facile (e comporta meno rischi) insultare o molestare online, perché le persone spesso si esprimono sotto la copertura dell’anonimato.

- Ha radici profonde.

Gli atteggiamenti e le tensioni sociali che suscitano sentimenti di odio online affondano le loro radici nella società, e non sono diversi, in genere, da quelli che alimentano il discorso dell’odio offline.

- Impunità e anonimato.

Sono le due presunte caratteristiche delle interazioni sociali in rete: l’impunità e l’anonimato. Queste abbassano le remore etiche. In realtà, però, qualsiasi azione compiuta sul web consente di rintracciare il suo autore.

**Come riconoscerlo?**

Il discorso dell’odio si manifesta con un ampio spettro di azioni: sebbene tutte le espressioni che istigano all’odio meritino di essere classificate come esecrabili, ne esistono alcune che possono essere peggiori di altre. È utile, quindi, prendere in considerazione alcuni aspetti:

- Il contenuto e il tono

Certe espressioni di odio sono più estreme, utilizzano termini più insultanti e possono perfino istigare altri ad agire. All’altra estremità della scala, troviamo insulti più moderati o generalizzazioni eccessive, che presentano certi gruppi o individui sotto una cattiva (e perfino sotto falsa) luce.

- L’intenzione degli autori degli insulti

Ci può capitare di offendere gli altri senza volerlo, e poi di pentircene, e perfino di ritirare quanto abbiamo detto.

- I bersagli o i bersagli potenziali

Alcuni gruppi, o individui, possono essere più vulnerabili di altri alle critiche. Può dipendere dal modo in cui sono globalmente considerati nella società, o da come sono rappresentati nei media, oppure dalla loro situazione personale, che non permette loro di difendersi efficacemente.

- Il contesto

Il contesto di una particolare espressione di odio è legato talvolta a circostanze storiche e culturali specifiche. Può includere altri fattori, come il mezzo utilizzato e il gruppo preso di mira, le tensioni o i pregiudizi esistenti, l’autorità del suo autore, etc.

- L’impatto o l’impatto potenziale

L’impatto reale o potenziale esercitato sugli individui, sui gruppi o sull’insieme della società è una delle principali considerazioni da tenere presenti. Spesso, le ripercussioni negative subite dall’individuo o dal gruppo si rivelano più importanti della valutazione dell’episodio da parte di osservatori esterni.

**Come intervenire?**

Lo sviluppo delle competenze digitali e l’educazione ad un uso etico e consapevole delle tecnologie assumono quindi un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete.

Occorre in tal senso fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, e promuovere la partecipazione civica e l’impegno, anche attraverso i media digitali e i social network.

Si potrebbe, quindi, pensare ad attività di analisi e produzione mediale, finalizzate soprattutto a:

- 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.

# 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 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.

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

- Dominanza. L'attività domina i pensieri ed il comportamento del soggetto, assumendo un valore primario tra tutti gli interessi.

- Alterazioni del tono dell'umore. L'inizio dell'attività provoca cambiamenti nel tono dell'umore. Il soggetto prova un aumento d'eccitazione o maggiore rilassatezza come diretta conseguenza dell'incontro con l'oggetto della dipendenza.

- Conflitto. Conflitti inter-personali tra il soggetto e coloro che gli sono vicini, conflitti intra- personali interni a se stesso, a causa del comportamento dipendente.

- Ricaduta. Tendenza a ricominciare l'attività dopo averla interrotta.

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

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

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

1. il giocatore è assorbito totalmente dal gioco;

2. il giocatore è preoccupato e ossessionato dal gioco;

3. Il gioco consente alla persona di sfuggire alla realtà con la sperimentazione di emozioni più piacevoli;

4. il giocatore manifesta sempre di più l'impulso di giocare e di sperimentare emozioni positive;

5. il giocatore sente di dover dedicare più tempo ai giochi;

6. il giocatore se non può giocare manifesta ansia, depressione e irritabilità;

7. può emergere un ritiro sociale;

8. il giocatore, anche se comprende la gravità della situazione e sospende di giocare comunque non riesce a interrompere del tutto;

9. il giocatore mente agli altri sull'utilizzo che fa dei giochi on line;

10. il giocatore ha perso o mette a rischio relazioni o opportunità a causa dei giochi su Internet o ha perso interesse verso attività nella vita reale.

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

La tecnologia infatti ha modificato gli ambienti in cui viviamo e ha un impatto sulla qualità della vita. Gli elementi che contribuiscono al benessere digitale sono:

- la ricerca di equilibrio nelle relazioni anche online;

- l'uso degli strumenti digitali per il raggiungimento di obiettivi personali;

- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile;

- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche).

Se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi. Strutturare regole condivise e stipulare con loro una sorta di "patto" d'aula e, infine, proporre delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d'aula (Es. adoperando la LIM o il dispositivo personale). È importante, quindi, non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli studenti e delle studentesse, stabilendo chiare e semplici regole di utilizzo.

---

# *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.

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

I contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di "revenge porn" letteralmente "vendetta porno" fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte (la Legge 19 luglio 2019 n.

69, all'articolo 10 ha introdotto in Italia il reato di revenge porn,con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti. Si veda l'articolo 612 ter del codice penale rubricato "Diffusione illecita di immagini o video sessualmente espliciti".)

Tra le caratteristiche del fenomeno vi sono principalmente:

- la fiducia tradita: chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo, inoltre, alla motivazione della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale);

- la pervasività con cui si diffondono i contenuti: in pochi istanti e attraverso una condivisione che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso a un numero esponenziale e infinito di persone e ad altrettante piattaforme differenti. Il contenuto, così, diventa facilmente modificabile, scaricabile e condivisibile e la sua trasmissione è incontrollabile;

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

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

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

---

# *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.

Potenziali vittime dell'adescamento online possono essere sia bambini che bambine, sia ragazzi che ragazze. Il fenomeno, infatti, non conosce distinzione di genere. Gli adolescenti sono particolarmente vulnerabili, poiché si trovano in una fase della loro vita in cui è molto importante il processo di costruzione dell'identità sessuale. Anche per questo potrebbero essere aperti e curiosi verso nuove esperienze e, talvolta, attratti da relazioni intime e apparentemente rassicuranti. In questa fase è importante, infatti, il bisogno di avere attenzioni esclusive da un'altra persona, di ottenere rinforzi esterni di approvazione per il proprio corpo e la propria immagine. È proprio in ragione della fiducia costruita nella relazione che le vittime di adescamento online riferiscono di sentirsi umiliate, usate, tradite e tendono a sentirsi in colpa e ad autosvalutarsi per essere cadute nella trappola.

L'adescamento, quindi, non avviene apparentemente con una dinamica violenta, ma il "prendersi cura" del minore rappresenta la conditio per carpirne la fiducia ed instaurare una relazione a sfondo erotico. Può capitare che l'adescatore si presenti al minore sotto falsa identità, fingendo quindi di essere un'altra persona così da attirare maggiormente l'attenzione del minore (ad esempio, potrebbe fingersi un talent scout del mondo dello spettacolo alla ricerca di volti nuovi).

Secondo una ricerca condotta da Ipsos per Save the Children Italia (2017) dal titolo "Che genere di tecnologie. Ragazze e digitale fra opportunità e rischi", il 42% delle ragazze fra i 12 e i 17 anni chatta spesso/sempre con qualcuno conosciuto in Internet e il 14,5% scopre che qualcuno con cui si è entrati in contatto in Internet non era la persona che diceva di essere. Piuttosto preoccupanti, inoltre, i dati sull'opinione delle ragazze fra i 12 e i 17 anni in relazione alla condivisione di materiale intimo e riservato online, destinato a rimanere fra una cerchia ristretta di persone.

Il 25,9% delle ragazze pensa che "è sempre sicuro, tanto lo fanno tutti», mentre il 40,3% pensa che "anche se non è sicuro, a volte non hai scelta".

**Le fasi dell'adescamento**

Il processo di adescamento segue generalmente 5 fasi:

1. Fase dell'amicizia iniziale: Questa è la fase in cui l'adescatore cerca i primi contatti con la vittima individuata, provando a socializzare con lei. Tenterà, quindi, di conoscerla meglio al fine di scoprirne bisogni, interessi e il contesto in cui vive. Condividendo argomenti di interesse del minore l'adescatore cercherà pian piano di conquistarsi la sua fiducia, ponendogli domande frequenti che attestano interesse e attenzione nei suoi confronti. Gradualmente affronterà con la vittima argomenti sempre più privati ed intimi.

2. La fase di risk-assessment: in seguito ai primi contatti con il minore, l'adescatore cerca di comprendere il contesto in cui si svolge l'interazione (es. da dove si collega alla Rete? I genitori lo controllano quando chatta? Che rapporto ha con loro?). L'obiettivo dell'adescatore è quello di rendere sempre più privato ed "esclusivo" il rapporto, cercando di passare, ad esempio, da una chat pubblica ad una privata, da una chat alle conversazioni attraverso il telefono, per poterne così carpire il numero.

3. Fase della costruzione del rapporto di fiducia: le confidenze e le tematiche affrontate divengono via via più private e intime o comunque molto personali. In questa fase l'adescatore può iniziare a fare regali di vario tipo alla vittima e può anche avvenire lo scambio di foto, subito e non necessariamente a sfondo sessuale.

4. Fase dell'esclusività: l'adescatore rende la relazione con il minore sempre più "segreta", isolandolo sempre più dalla famiglia e dagli amici. Chiederà alla vittima di non raccontare a nessuno ciò che sta vivendo. L'esperienza reciproca verrà presentata come un "geloso segreto" da custodire per non rovinare tutto. In questa fase l'adescatore potrà ricorrere a ricatti morali puntando sulla fiducia costruita, sulla paura o sul senso di colpa.

5. Fase della relazione sessualizzata: in questa fase la richiesta di immagini o video sempre più privati e a sfondo erotico potrebbe essere più insistente, così come la proposta di incontri offline. Qualora il minore avesse già inviato immagini o video privati, potrebbe essere ricattato dall'adescatore: se non accettasse un eventuale incontro l'adescatore potrebbe diffondere quel materiale online. Questi, inoltre, tenderà a presentare sempre la situazione come "normale" al fine di vincere le eventuali resistenze del minore a coinvolgersi in tale rapporto.

**Come riconoscerlo?**

Per riconoscere un eventuale caso di adescamento online è importante prestare attenzione a piccoli segnali che possono essere indicatori importanti, come ad esempio un cambiamento improvviso nel comportamento di un minore. A seguire, alcuni segnali e domande che potrebbero esserci di aiuto:

- Il minore ha conoscenze sessuali non adeguate alla sua età?

- Venite a conoscenza di un certo video o di una foto che circola online o che il minore ha ricevuto o filmato, ma c'è imbarazzo e preoccupazione nel raccontarvi di più…

- Il minore si isola totalmente e sembra preso solo da una relazione online?

- Ci sono prese in giro e allusioni sessuali verso un bambino/ragazzo in particolare?

**L'importanza di un'adeguata educazione all'affettività e alla sessualità**

Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto 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. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e perché no, della sessualità.

Nella società digitale, attraverso la Rete, i minori definiscono se stessi, si raccontano e sperimentano nuove forme di identità, socializzano, si emozionano e si relazionano con gli altri, scoprono la propria sessualità e giocano con essa.

Tutto ciò risponde a bisogni assolutamente naturali e importanti, ma allo stesso tempo può esporre i ragazzi a possibili rischi come quello,appena approfondito, dell'adescamento online.

Il desiderio di conferma sociale (da ottenere anche attraverso i social) e, talvolta, la scarsa consapevolezza degli adolescenti nel gestire la propria immagine online quando pubblicano sui loro profili social video e foto piuttosto intimi o sensuali, può aumentare il rischio di esporli ad un adescamento online. Con un'adeguata competenza digitale ed emotiva, Internet potrebbe essere un valido supporto per i ragazzi e le ragazze nel loro percorso di esplorazione della sessualità. Purtroppo, però, non è sempre così. La Rete, infatti, abbonda di contenuti inadeguati che offrono una rappresentazione distorta della sessualità e dei rapporti uomo-donna. La sessualità in Rete è spesso rappresentata in modo decontestualizzato e senza alcun richiamo alla dimensione affettiva ed emotiva dei soggetti. Il più delle volte,tali rappresentazioni ricalcano con forza stereotipi di genere come quello della "donna oggetto" e quello dell'"uomo forte e virile", tanto più forte e virile quanto più è in grado di conquistare e dominare quell'"oggetto".

In un contesto simile non c'è da stupirsi se, talvolta, anche i comportamenti degli adolescenti in Rete nella gestione della propria sessualità o semplicemente della

propria immagine online riproducano tali modelli. Modelli che la società odierna sembra tuttora confermare in numerosi messaggi che quotidianamente ci arrivano attraverso i media.

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

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

**Come intervenire?**

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.

I minori vittime di adescamento riferiscono, generalmente, di sentirsi traditi, ma anche di provare un senso di colpa per essere caduti in trappola ed essersi fidati di uno sconosciuto.

Inutile sottolineare che nei casi più estremi in cui l'adescamento porta ad un incontro fisico e ad un abuso sessuale un sostegno psicologico esperto per il minore è da considerarsi prioritario e urgente.

Per consigli e per un supporto è possibile rivolgersi alla Helpline di Generazioni Connesse (19696): operatori esperti e preparati sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che dei bambini, degli

adolescenti, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti l'utilizzo dei nuovi media.

---

# *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.**

Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia. L'intento è quello di facilitare il processo di rimozione del materiale stesso della rete e allo stesso tempo consentire le opportune attività investigative finalizzate ad identificare chi possiede quel materiale, chi lo diffonde e chi lo produce, ma, soprattutto e primariamente, ad identificare i minori abusati presenti nelle immagini e video, assicurando la fine di un abuso che potrebbe essere ancora in corso e il supporto necessario.

Parallelamente, per salvaguardare il benessere psicofisico degli alunni coinvolti nella visione di questi contenuti, sarà opportuno ricorrere ad un supporto psicologico anche passando per una consultazione presso il medico di base o pediatra di riferimento. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza: Consultori Familiari, Servizi di Neuropsichiatria Infantile, centri specializzati sull'abuso e il maltrattamento all'infanzia, etc.

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

Studi in materia dimostrano come l'utilizzo di materiale pedopornografico possa essere propedeutico all'abuso sessuale agito ed è quindi fondamentale, in termini preventivi, intervenire per ridurre l'incidenza di tale possibilità. L'abuso sessuale online rappresenta una particolare declinazione dell'abuso sessuale su bambini/e, la cui caratteristica fondante è il ruolo ricoperto dalle tecnologie digitali, le quali diventano il mezzo principale attraverso cui l'abuso viene perpetrato, documentato e diffuso in Rete con immagini e/o video. Le dinamiche attraverso cui l'abuso sessuale online si manifesta producono effetti sulle vittime che si aggiungono e si moltiplicano a quelli associati all'abuso sessuale.

La scuola quindi ha l'obbligo di dotarsi di una guida procedurale con tutte le modalità di identificazione; deve individuare gli interventi e mettere a disposizione strumenti alternativi.

Il ruolo degli insegnanti è quello di essere buoni osservatori e comprendere i segnali

che gli allievi mandano. Fondamentale è l'apertura di un canale comunicativo sicuro e orientato alla sensibilizzazione.

## Il nostro piano d'azioni

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

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

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

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

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/ studentesse.

- Organizzare uno o più incontri informativi per la prevenzione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

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

# 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 si segnaleranno:

- 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 ovideo imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per unpubblico 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.

Tutte le segnalazioni riportate dai docenti verranno registrate su apposita scheda (diario di bordo, messo a disposizione dei docenti).

---

# *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.

E’ opportuno sottolineare che la rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti. Perciò è fondamentale una corretta informazione/formazione e una sensibilizzazione di tutti gli adulti coinvolti.

Il personale scolastico, soprattutto nella componente docente, ma anche in quella del personale ATA, è invitato ad evitare atteggiamenti accusatori o intimidatori, in modo tale da riuscire a ricevere dai minori più fragili segnalazioni e confidenze circa situazioni problematiche vissute. E’ fondamentale, infatti, osservare per tempo ciò che accade, per poter agire immediatamente nei confronti di atti non opportuni e in modo tale da poter scongiurare conseguenze a lungo termine ben più gravi, in quanto negative per il benessere e la crescita armonica dei minori coinvolti. La gestione dei casi rilevati andrà differenziata a seconda della loro gravità; è in ogni caso opportuna la condivisione a livello di Consiglio di Classe/Team di Docenti di ogni episodio rilevato. Alcuni avvenimenti di lieve rilevanza possono essere affrontati e risolti con la discussione collettiva in classe. Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e

individuare una strategia comune per affrontarlo e rimediare. Per i casi più gravi bisogna informare il Dirigente Scolastico che nel caso di reati veri e propri effettuerà la denuncia all'autorità giudiziaria.

**Come segnalare eventuali casi**

Il personale della scuola, anche con l'ausilio del personale di assistenza tecnica e dell'Animatore digitale, dovrà provvedere 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, il Dirigente Scolastico e, ove si configurino reati, la Polizia Postale. In ogni caso, sarà opportuna una tempestiva informazione delle famiglie in merito all'accaduto, anche per consentire ulteriori indagini e, in assenza di prove oggettive, di raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico ed, eventualmente, alla Polizia Postale. Qualora siano coinvolti più alunni, in qualità di vittime o di responsabili della condotta scorretta, le famiglie degli alunni in questione saranno informate tempestivamente per un confronto. In base all'entità dei fatti si provvederà:

1) a una comunicazione scritta tramite diario alle famiglie;

2) a una nota disciplinare sul registro di classe;

3) a una convocazione formale dei genitori degli alunni, tramite segreteria;

4) 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.

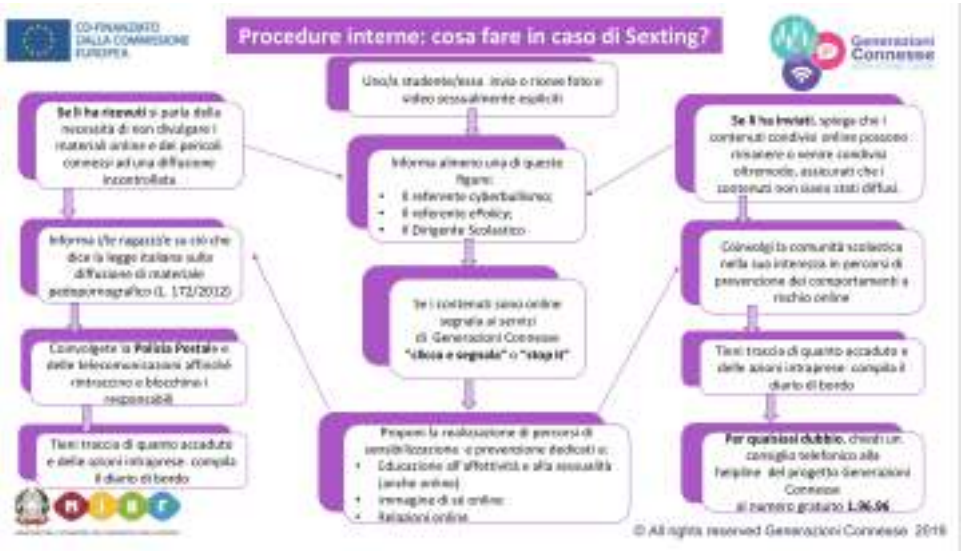
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

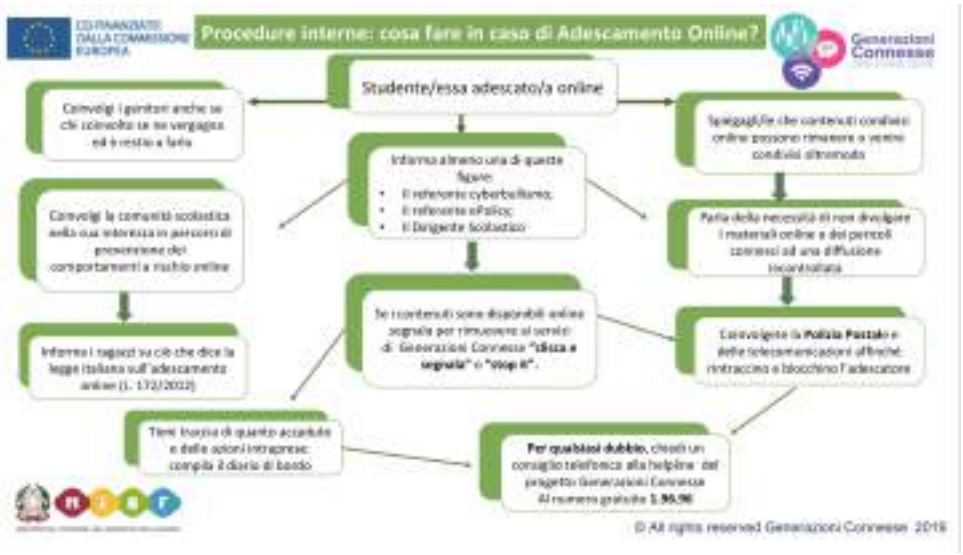
## Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



## 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 per la collaborazione sinergica tra scuola- famiglia - servizi territoriali, al fine di creare un modello compositivo e lineare di azioni condivise:

- coinvolgimento di tutti gli attori della scuola: studenti e studentesse, docenti, genitori e personale ATA, per l'affermazione di un modello di scuola come comunità;

- 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, come Polizia postale ed ATS per servizi specialistici;

- promozione dell'educazione al rispetto;

- sviluppo del pensiero critico;

- promozione dell’Educazione Civica Digitale.