MINISTERO DELL'ISTRUZIONE E DEL MERITO
ISTITUTO COMPRENSIVO STATALE
"F. BERNAGOZZI"
Scuola dell'Infanzia – Scuola Primaria – Scuola Secondaria di 1° grado
Piazza XX settembre, 17 - 44015 Portomaggiore – Tel. (0532) 811048
e-mail: feic824002@istruzione.it PEC: feic824002@pec.istruzione.it C.F. 93085160385

DOCUMENTO DI e-Policy

Redatto dal Team per la prevenzione del bullismo e del cyberbullismo



Capitolo 1

Introduzione al documento di e-Policy

1.1 - Scopo dell'e-Policy

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 (TIC o 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'e-Policy**
    - Scopo dell'e-Policy
    - Ruoli e responsabilità
    - Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto

- Condivisione e comunicazione dell'e-Policy all'intera comunità scolastica
- Gestione delle infrazioni alla e-Policy
- Integrazione dell'e-Policy con regolamenti esistenti
- Monitoraggio dell'implementazione dell'e-Policy e suo aggiornamento

2. Formazione e curricolo

- Curricolo sulle competenze digitali per gli studenti
- Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
- Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
- Sensibilizzazione delle famiglie e Patto di corresponsabilità

3. Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola

- Protezione dei dati personali
- Accesso ad Internet
- Strumenti di comunicazione online
- Strumentazione personale

4. Rischi on line: conoscere, prevenire e rilevare

- Sensibilizzazione e prevenzione
- Cyberbullismo: che cos'è e come prevenirlo
- Hate speech: che cos'è e come prevenirlo
- Dipendenza da Internet e gioco online
- Sexting

- Adescamento online
- Pedopornografia

5. Segnalazione e gestione dei casi

a. Cosa segnalare

b. Come segnalare: quali strumenti e a chi

c. Gli attori sul territorio per intervenire

d. 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.
Finalità del presente documento è regolamentare in modo organico e condiviso dall'intera Comunità Scolastica i comportamenti e le procedure in merito all'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC) nella didattica, promuoverne un uso critico e consapevole, prevenire, rilevare, gestire e contrastare le problematiche derivanti da un uso ignaro ed improprio delle tecnologie digitali. Il nostro Istituto riconosce che le TIC rappresentano una grande opportunità per sostenere l'insegnamento, promuovere la creatività, stimolare la consapevolezza e migliorare l'apprendimento degli studenti, ma è conscio dei rischi relativi e della conseguente necessità di fronteggiarli adeguatamente.

In particolare si perseguono i seguenti scopi:

- Stabilire i principi fondamentali rispetto all'uso delle TIC; Tutelare gli allievi e tutto il personale;
- Operare in modo sicuro e responsabile con Internet e altre tecnologie informatiche e di comunicazione;
- Avviare ad un uso accettabile e responsabile di Internet a scopo didattico, da estendere anche al di fuori dell'ambito scolastico;

- Elaborare procedure chiare e condivise per affrontare un uso improprio degli strumenti digitali o gli abusi online come il cyberbullismo;

- Monitorare le procedure;

- Assicurarsi che tutti i membri della comunità scolastica siano consapevoli del fatto che i comportamenti illeciti o pericolosi sono ritenuti inaccettabili e che verranno intraprese azioni appropriate, disciplinari e/o giudiziarie quando la situazione lo richiederà.

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.

Ruoli e responsabilità chiave del Dirigente Scolastico

- Garantire la sicurezza online dei membri della comunità scolastica;

- Accertarsi che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro e delle differenze, un utilizzo positivo e responsabile delle TIC;

- Promuovere il monitoraggio ed il controllo interno della sicurezza online;

- Conoscere le procedure da seguire in caso di un grave incidente di sicurezza online;

- Valutare il rischio nell'uso di strumenti e TIC, in modo che quanto programmato possa soddisfare le istanze educative e didattiche dichiarate nel PTOF di Istituto;

- Assicurare che il sito web della scuola includa informazioni sulla cultura della sicurezza online, rilevanti e condivise.

Dirigente Scolastico con DSGA (gestori dati e informazioni)

- Assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnologica della scuola sia funzionante, sicura, non aperta ad uso improprio o a dannosi attacchi esterni;

- Favorire il funzionamento dei diversi canali di comunicazione all'interno della scuola e fra la scuola e le famiglie;

- Garantire che i dati di gestione siano accurati e aggiornati;

- Promuovere le migliori pratiche nella gestione delle informazioni, ossia mettere in atto un sistema di controllo di accesso appropriato (i dati sono utilizzati, trasferiti e cancellati in linea con i requisiti di protezione dei dati);

- Mantenere i controlli di accesso per proteggere le informazioni sensibili archiviati su dispositivi di proprietà della scuola.

Animatore e Team digitale

- Stimolare la formazione interna negli ambiti di sviluppo della scuola digitale e fornire consulenza e informazioni al personale in relazione ai rischi online ed alle misure di prevenzione e gestione degli stessi;

- Monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola;

- Assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate;

- Curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti;

- Coinvolgere la comunità scolastica nella partecipazione ad attività e progetti attinenti la scuola digitale;

- Inserire l'educazione all'uso consapevole delle TIC e alla sicurezza online all'interno del curricolo di studi;

- Collaborare con il personale tecnico esterno in forza alla scuola.

Referente bullismo e cyberbullismo (ed eventuale gruppo di lavoro)

- Prendere parte ai corsi di formazione ai fini di garantire l'acquisizione di idonee competenze teoriche e pratiche;

- Pubblicizzare attività formative per i docenti;

- Favorire la conoscenza del fenomeno e gli strumenti di prevenzione dello stesso affinché le famiglie possano riconoscerlo ed intervenire in modo corretto;

- Sostenere le famiglie e i minori vittime del cyberbullismo;

- Promuovere, in collaborazione con tutti gli insegnanti, l'educazione all'uso consapevole della rete di bambini e ragazzi, favorendo specifici percorsi didattici finalizzati a responsabilizzare gli stessi minori e a promuovere la consapevolezza in ordine ai rischi, oltre che alle opportunità.

Docenti

- Aderire alla e-Policy;
- Educare alla sicurezza online nello svolgimento della propria disciplina;
- Supervisionare e guidare gli alunni quando sono impegnati in attività di apprendimento che coinvolgono tecnologie online;
- Assicurarsi che gli alunni siano capaci di ricercare contenuti online in sicurezza e siano consapevoli dei problemi relativi ai contenuti elettronici (come ad esempio le leggi sul copyright).

Alunni

- Leggere, capire e aderire alla e-Policy;
- Essere responsabili, in relazione al proprio grado di maturità e di apprendimento, nell'utilizzare i sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- Comprendere le potenzialità offerte dalle TIC per la ricerca di contenuti e materiali, ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;
- Capire l'importanza di segnalare l'abuso, l'uso improprio o l'accesso a materiali inappropriati;
- Sapere quali azioni intraprendere in caso di vulnerabilità propria o altrui quando si utilizza la tecnologia online;
- Comprendere l'importanza di adottare sempre comportamenti sicuri e buone pratiche di sicurezza online quando si usano le tecnologie digitali e essere consapevoli che la policy di sicurezza online della scuola può aiutarli anche in ambito extrascolastico;
- Adottare comportamenti rispettosi nella comunicazione in rete osservando la *netiquette*.

Genitori

- Leggere la e-Policy;
- Consultarsi con la scuola se si hanno preoccupazioni circa l'uso della tecnologia online o offline da parte dei loro figli;
- Seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllando l'utilizzo dei dispositivi digitali e di internet;
- Sostenere la scuola nel promuovere la sicurezza online;
- Concordare le modalità d'uso di dispositivi personali, di Internet attraverso la rete di Istituto;

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, ecc.) 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).

1.4 - Condivisione e comunicazione dell'e-Policy 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/alle 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.

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.
La e-Policy sarà comunicata al personale/alunni/comunità e persone che usufruiscono del servizio di istruzione/educazione nei seguenti modi:

- Sul sito della scuola;
- Nella sezione "Bacheca" del Registro elettronico;

1.5 - Gestione delle infrazioni alla e-Policy

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. Le sanzioni, riferite soprattutto agli alunni, *avranno come carattere preferenziale quello educativo/riabilitativo* e in ogni caso *verrà coinvolta la componente genitori*, in qualità di primi educatori.
Le infrazioni saranno riferite direttamente al Dirigente Scolastico. La scuola adotterà tutte le misure necessarie per garantire agli studenti l'accesso a materiale e ambienti appropriati, anche se è impossibile evitare in assoluto che essi trovino materiale indesiderato navigando in rete a scuola. La scuola non può farsi carico della responsabilità per il materiale trovato su internet o per eventuali conseguenze causate dall'accesso ad internet. Qualsiasi sospetto, rischio, uso improprio, violazione va segnalato immediatamente al Dirigente che, eventualmente, riferisce direttamente alle autorità di competenza. Al personale, agli studenti e agli altri componenti della comunità scolastica sono date informazioni sulle infrazioni previste e le eventuali sanzioni.

1.6 - Integrazione dell'e-Policy con Regolamenti esistenti

Il Regolamento d'Istituto viene aggiornato con specifici riferimenti all'e-Policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida MIM e le indicazioni normative generali sui temi in oggetto. La e-Policy fa riferimento e si armonizza con tutti gli altri regolamenti vigenti nell'Istituto, in particolare con Regolamento d'Istituto. Integra tali regolamenti costituendo la sezione relativa all'uso delle nuove tecnologie, dei nuovi ambienti di apprendimento e delle

metodologie didattiche offerti dall'Istituto (scuola 3.0, ecc.).
Tutto ciò che qui non è normato è da considerarsi regolamentato secondo la disciplina generale.

1.7 - Monitoraggio dell'implementazione della e-Policy e suo aggiornamento

L'e-Policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

Il nostro piano d'azione

Azioni da svolgere entro un'annualità scolastica:

- Diffondere la conoscenza del progetto "Generazioni connesse" e di altre risorse on line per la lotta al bullismo e al cyberbullismo presso i docenti;
- Svolgere attività di sensibilizzazione e diffondere una cultura di prevenzione presso le famiglie;
- Sensibilizzare alunni e alunne verso le tematiche in oggetto mediante attività didattiche, ludiche ed informative; includendo progetti con eventuale personale esterno.

Azioni da svolgere nei prossimi 3 anni:

- Promuovere la conoscenza del documento di e-Policy presso alunni e alunne, docenti e famiglie.

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.
La competenza digitale, per la sua importanza nelle attività professionali e anche quotidiane, è ritenuta dall'Unione Europea una competenza chiave per lo sviluppo del senso di cittadinanza. Nel curricolo disciplinare del nostro Istituto tale competenza pervade in modo trasversale i vari insegnamenti; questa declinazione scaturisce dalla necessità di iniziare a dare una formazione di base sull'uso delle TIC, inserendole nelle attività didattiche, per arrivare nelle classi finali a fornire gli strumenti per un approccio consapevole, critico, autonomo e responsabile. Tali competenze sono oggetto di certificazione, come da apposito documento ministeriale, al termine della scuola Primaria e Secondaria. Negli ultimi anni la scuola ha provveduto all'implementazione della dotazione digitale dei vari plessi, anche attraverso la partecipazione ai progetti PON, per consentire l'introduzione di metodologie basate sull'uso delle TIC.

2.2 - Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica

È fondamentale che tutti i docenti 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.

I docenti, in conformità con quanto previsto dal Piano triennale dell'offerta formativa, hanno partecipato a corsi di formazione nell'ambito di piani nazionali e ad iniziative organizzate dall'istituzione o dalle scuole associate in rete incrementando le competenze digitali di base. I docenti del team digitale stanno seguendo la formazione ad essi destinata, che si auspica sia spendibile all'interno dell'Istituto. Inoltre i docenti potranno avvalersi dei corsi di aggiornamento promossi dall'Ambito Territoriale oppure presenti sulla piattaforma SOFIA riguardanti l'innovazione didattica e la didattica digitale.

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 verranno organizzati dall'Istituto scolastico con la collaborazione, se necessario, di personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, ecc.), delle

amministrazioni comunali, dei servizi socio-educativi, delle associazioni presenti, delle occasioni formative promosse dal PNRR. La formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet può prevedere momenti di auto-aggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi.

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'e-Policy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di Corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

L'Istituto ha promosso e continua a promuovere iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle situazioni di rischio online. Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo. Sul sito scolastico e sulla bacheca virtuale relativa a "Generazioni connesse" saranno messi in condivisione materiali dedicati ad alunni e alle famiglie come guide in formato pdf e video che possono fornire spunti di approfondimento e confronto. La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento (e-Policy) per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e prevenire i rischi legati a un utilizzo non corretto di internet.

Il nostro piano d'azione

Azioni da sviluppare nell'arco dell'anno scolastico 2025/2026

- Organizzare per i docenti incontri con esperti sulle competenze digitali;
- Organizzare per gli alunni e le alunne incontri con associazioni, esperti e/o forze dell'ordine sull'utilizzo consapevole dei dispositivi digitali ed i pericoli della rete;
- Organizzare per gli alunni e le alunne incontri con associazioni, esperti e/o forze dell'ordine sulla sensibilizzazione ai temi del bullismo e del cyberbullismo.

Azioni da sviluppare nell'arco dei tre anni scolastici successivi

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica e sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali;

- Promuovere per il corpo docente incontri informativi 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 per i docenti incontri con esperti sulle competenze digitali;

- Organizzare per i genitori incontri con esperti 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. In questo paragrafo dell'e-Policy 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 rende disponibili i modelli di liberatoria da utilizzare, conformi alla normativa vigente in materia di protezione dei dati personali.

Per il trattamento dei dati personali si fa riferimento al Decreto legislativo 30 giugno 2003, n. 196 e al GDPR Regolamento EU 679/2016. Nello specifico si possono individuare alcune linee guida di e-safety:

- Si consiglia al personale scolastico di non condividere i propri contatti telefonici e e-mail personali, salvo in occasione di particolari eventi (es. viaggi di istruzione). Si caldeggia invece l'utilizzo dei contatti ufficiali della scuola;

- All'atto dell'iscrizione sarà richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso di immagini e video delle/dei minori per finalità strettamente connesse alla vita scolastica;

- Le fotografie o i video da pubblicare sul sito che includano allieve e allievi saranno selezionati tenendo conto dei consensi espressi dai genitori ad inizio anno scolastico.

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;*

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, costituita il 27 ottobre 2014 presso la Camera dei Deputati. 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.

Si progetta, con la collaborazione dell'assistenza tecnica esterna all'I.C., un piano di revisione del sistema di filtraggio presente nei vari plessi, così da evitare il più possibile l'accesso a siti inappropriati al contesto scolastico. Per quanto riguarda l'utilizzo di software antivirus si opta per l'utilizzo di programmi gratuiti, scegliendo quelli considerati dal personale tecnico più efficaci. Ai docenti appartenenti al gruppo di lavoro area multimedialità si affida il compito di mantenere costantemente aggiornati i suddetti software. Tutti coloro che utilizzano i supporti multimediali della scuola saranno sensibilizzati ad eseguire una scansione antivirus quando collegano dispositivi personali di archiviazione esterna. Quasi tutti i plessi dell'Istituto sono dotati di una rete wireless; ove possibile e conveniente (per es. laboratori di informatica) si procede alla connessione alla rete internet attraverso cavo. Resta necessario rivedere, in collaborazione con le amministrazioni comunali dei cinque paesi afferenti all'I.C., l'efficienza delle reti wireless, non sempre soddisfacente.

I dispositivi sono collegabili alla rete internet esclusivamente tramite password. Si ritiene utile che il personale docente di ogni plesso, o almeno un rappresentante di essi, sia a conoscenza della password di accesso, così da poter connettere facilmente tutti i dispositivi necessari per lo svolgimento delle attività didattiche. Nell'ottica di un maggior sviluppo del "Byod" (ossia l'utilizzo di dispositivi elettronici personali durante le attività didattiche), soprattutto nella scuola Secondaria di Primo Grado, si è fornita la password d'accesso alla rete dedicata anche agli alunni delle classi coinvolte.

3.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo

scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

Il Dirigente Scolastico, i Collaboratori vicari ed il personale di segreteria sono in possesso di un proprio indirizzo e-mail, utilizzabile dal personale della scuola per comunicazioni professionali. Anche ciascun plesso dell'I.C. dispone di un proprio indirizzo di posta elettronica. Il personale interno alla scuola (D.S., docenti, personale di segreteria) e i genitori hanno a disposizione la piattaforma di registro elettronico "Spaggiari" per comunicazioni "interne". L'Istituto ha chiesto l'iscrizione alla piattaforma G-Suite. Si tratta di un'applicazione di Google, nata come espansione cloud. La suite è uno strumento che consente l'utilizzo di molte applicazioni utili alla didattica, all'organizzazione delle attività in classe e alle comunicazioni tra utenti, infatti sulla piattaforma sono presenti programmi come simil-Word, Excel, PowerPoint, Outlook, ma anche altri che consentono la condivisione di file, il lavoro in team, la pianificazione e lo sviluppo della creatività.

Sito web della scuola

Il sito web della scuola (https://www.icportomaggiore.edu.it) è la prima e principale interfaccia dell'Istituto. Oltre alle informazioni generali e di contatto, vi si trovano apposite sezioni dedicate a docenti, personale ATA e famiglie degli alunni con informazioni, circolari, modulistica, presentazione di attività e progetti. La scuola, al momento, non dispone di un blog ma di un giornalino scolastico che viene pubblicato periodicamente sul sito.

Social network

L'Istituto Comprensivo è attivo sul social network Facebook per pubblicizzare le attività e l'offerta formativa della scuola. E' severamente vietato agli studenti e a tutto il personale della scuola la pubblicazione senza autorizzazione sui social network di immagini e/o video realizzati nel contesto scolastico che possano ledere la privacy dei soggetti coinvolti.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/delle 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 e-Policy 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. E' convinzione comune dei docenti dell'Istituto Comprensivo, che l'utilizzo delle TIC in ambito didattico debba essere valorizzato, educato, incentivato e orientato costruttivamente.

SCUOLA DELL'INFANZIA: i/le bambini/e non possono utilizzare a scuola cellulari o tablet personali. La connessione ad Internet, nelle aule e nei laboratori, è sempre supervisionata dagli insegnanti.

SCUOLA PRIMARIA: i/le bambini/e di tutte le classi non possono utilizzare a scuola cellulari o tablet personali. La connessione ad Internet nelle aule e nei laboratori è sempre supervisionata dagli insegnanti.

SCUOLA SECONDARIA: attualmente, solamente nelle classi 3.0, ed esclusivamente per fini didattici, è permesso l'utilizzo di strumenti personali per la navigazione in internet a scuola (PC, tablet); l'utilizzo è costantemente supervisionato dagli insegnanti. Per gli alunni e le alunne di tutte le altre classi tale impiego è vietato.

Il nostro piano di azione

Azioni da sviluppare nell'arco dell'anno scolastico 2025/2026 e dei tre anni successivi

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

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*.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

La legge n.70/2024 apporta alcune modifiche alla legge n.71/2017 sulla prevenzione e il contrasto al cyberbullismo.

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 sue successive modifiche) 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, PAI, RAV).

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 ecc.) 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, ecc.) 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. Data l'importanza di questa tematica l'Istituto promuoverà interventi di formazione degli studenti e delle studentesse tenuti dai docenti e da esperti esterni (forze dell'ordine, psicologi, personale sanitario...).

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. Data l'importanza di questa tematica l'Istituto promuoverà interventi di formazione degli studenti e delle studentesse tenuti dai docenti e da esperti esterni (forze dell'ordine, psicologi, personale sanitario...).

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.

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).

Data l'importanza di questa tematica l'Istituto promuoverà interventi di formazione degli studenti e delle studentesse tenuti dai docenti e da esperti esterni (forze dell'ordine, psicologi, personale sanitario...).

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 www.generazioniconnesse.it alla sezione "**Segnala contenuti illegali"** (Hotline).

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

Il nostro piano d'azioni

Azioni da sviluppare nell'arco dell'anno scolastico 2025/2026

- 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 per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse

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 piiù incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/alle studenti/studentesse, con il coinvolgimento di esperti;

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

- Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse;

- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale;

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

- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/alle studenti/studentesse;

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

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

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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 comunicazioni e/o circolari ufficiali, 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? ecc.). 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 ultra-quattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di **Helpline 19696** e **Chat di Telefono Azzurro** per supporto ed emergenze;

- **Clicca e segnala di Telefono Azzurro** e **STOP-IT di Save the Children Italia** per segnalare la presenza di materiale pedopornografico online.

5.2. - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative. Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.
Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

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

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

Strumenti a disposizione di studenti/esse

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

- indirizzi e-mail delle docenti del Team antibullismo dell'Istituto, a cui inviare 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 (periodicamente e/o su richiesta).

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

5.3. - Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi ad altre figure, enti, istituzioni e servizi presenti sul territorio qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.
Per una mappatura degli indirizzi di tali strutture è possibile consultare il **Vademecum** di Generazioni Connesse "*Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani"*, 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.

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.

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.

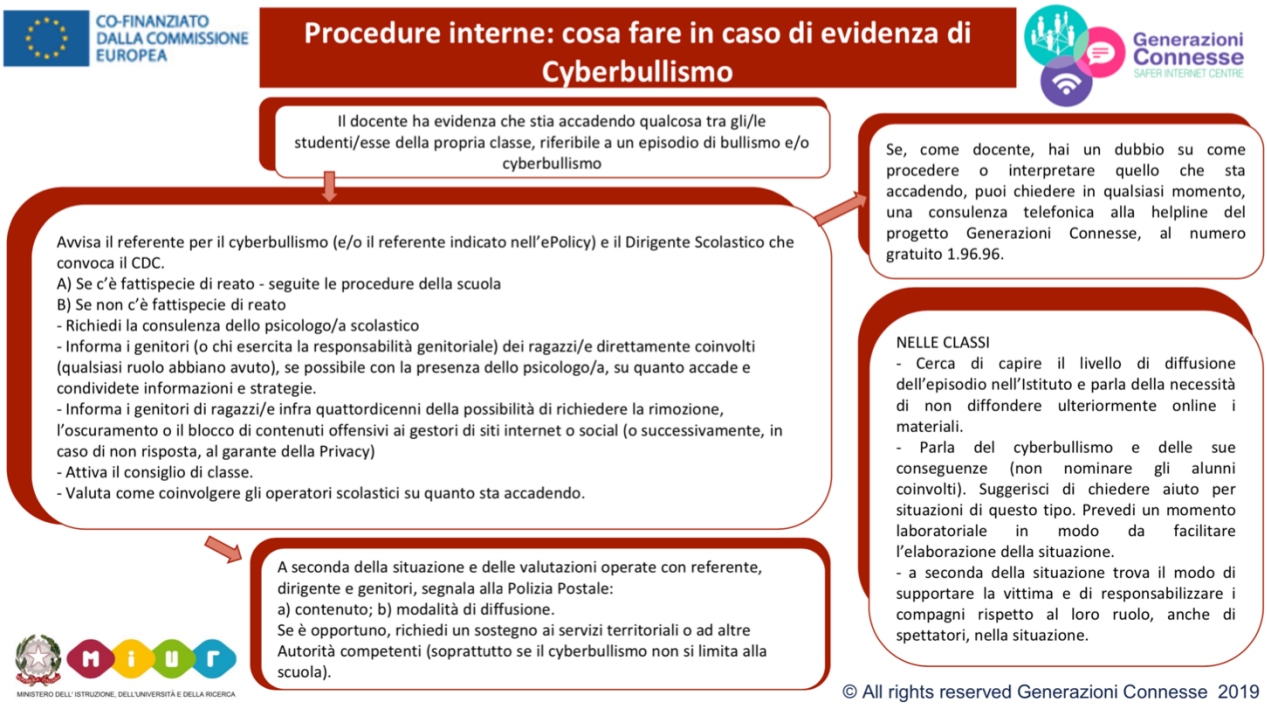
Aziende Sanitarie Locali: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete.

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.

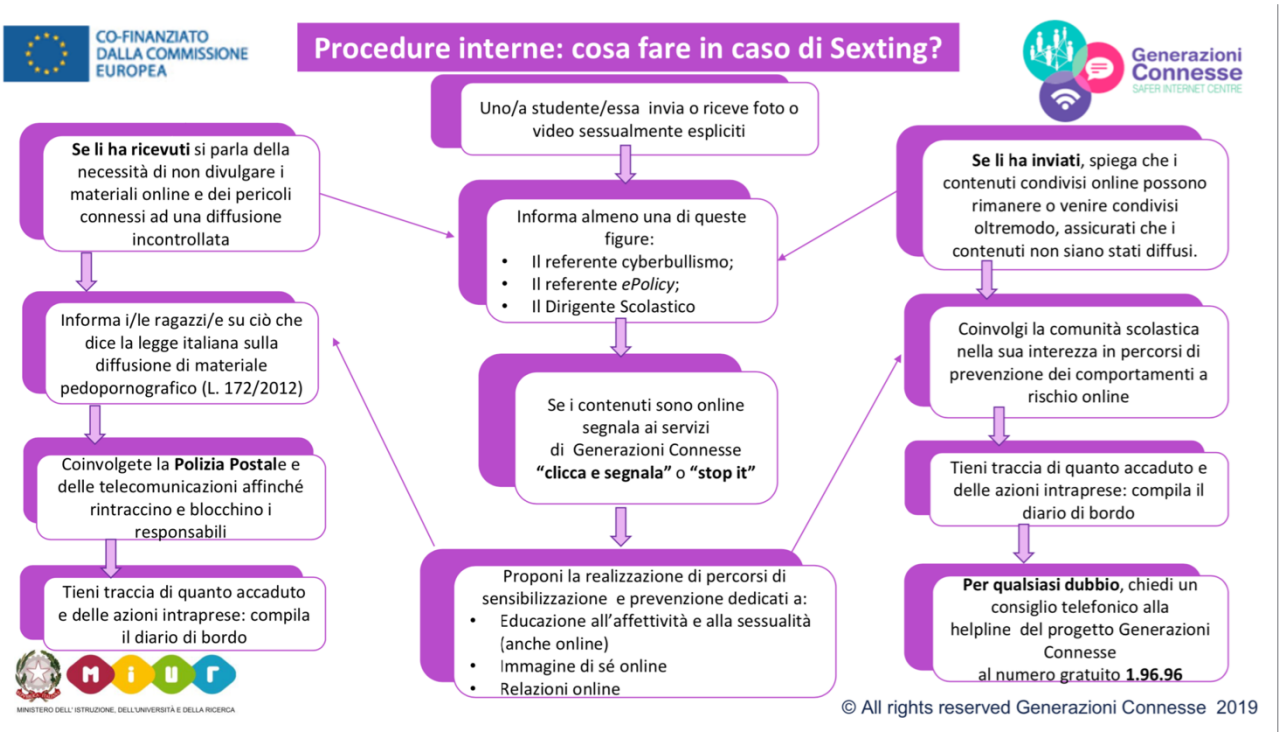
Tribunale per i Minorenni: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

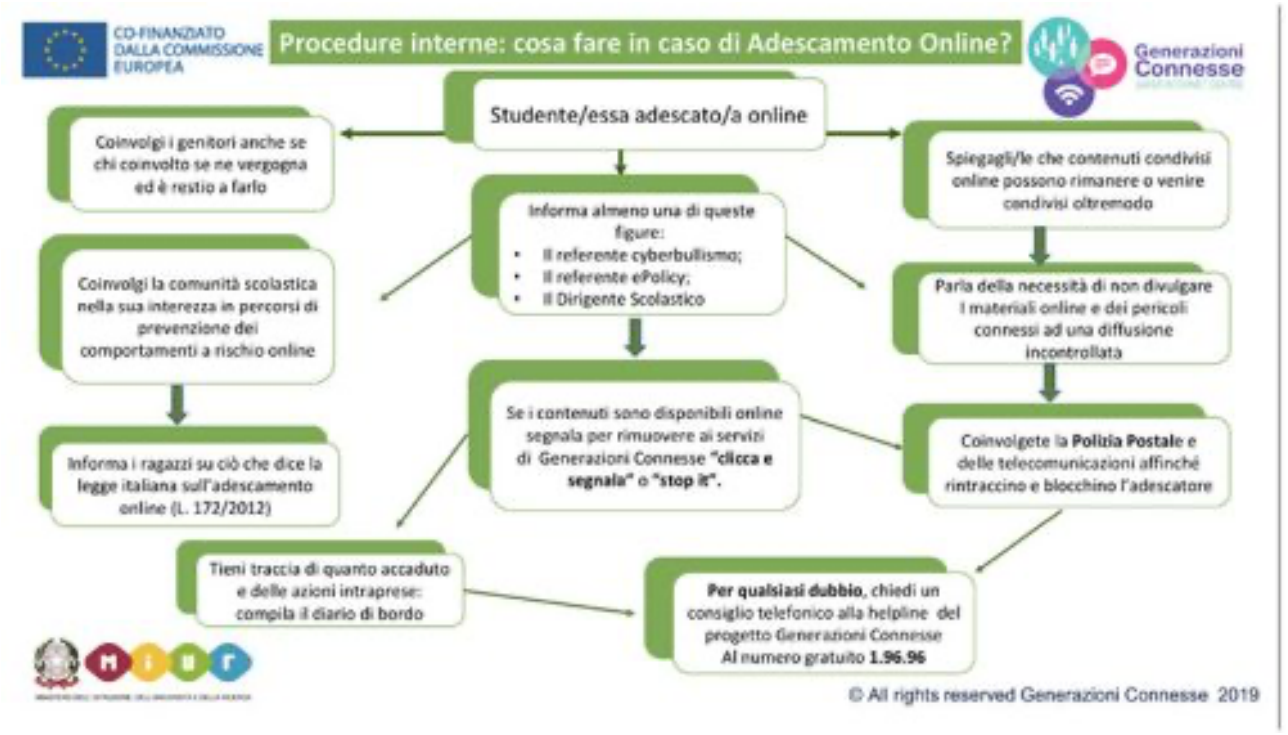
5.4. - Allegati con le procedure

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

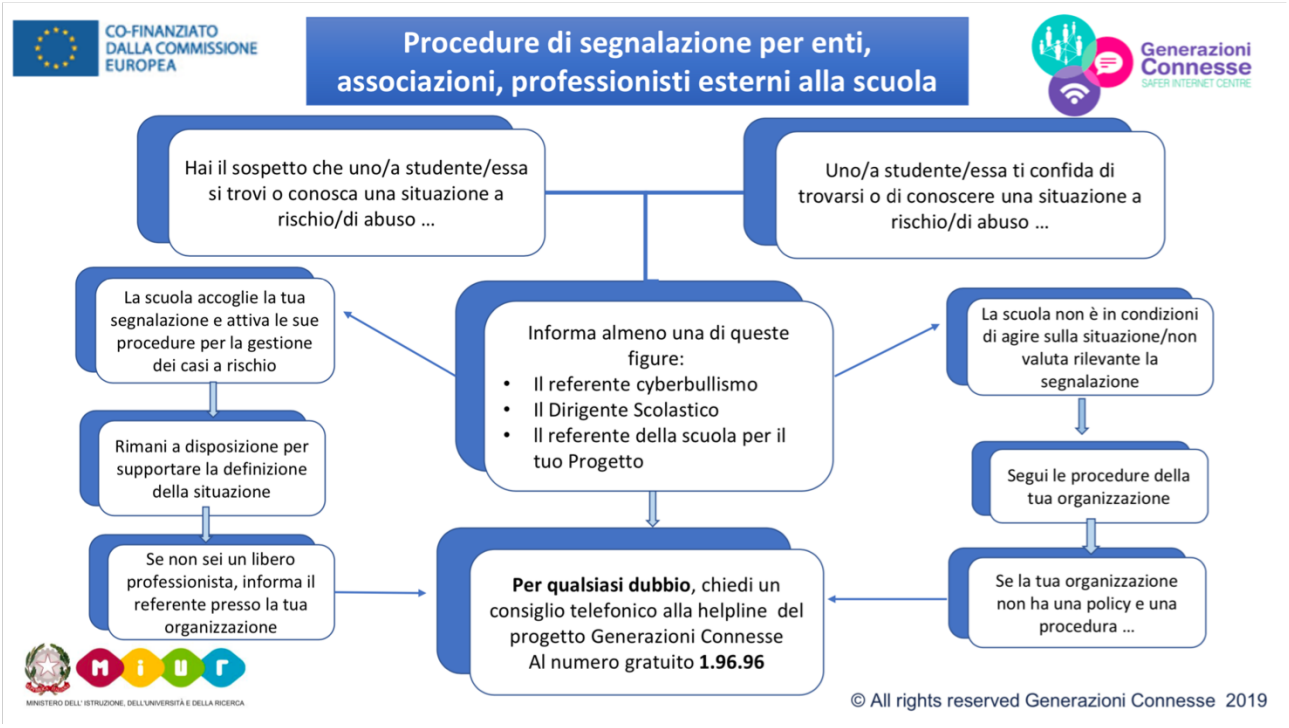





CO-FINANZIATO DALLA COMMISSIONE EUROPEA
Procedure interne: cosa fare in caso di Sexting?
Generazioni Connesse
SAFER INTERNET CENTRE
Uno/a studente/essa invia o riceve foto o video sessualmente espliciti
Se li ha ricevuti si parla della necessità di non divulgare i materiali online e dei pericoli connessi ad una diffusione incontrollata
Informa almeno una di queste figure:
• Il referente cyberbullismo;
• Il referente ePolicy;
• Il Dirigente Scolastico
Se li ha inviati, spiega che i contenuti condivisi online possono rimanere o venire condivisi oltremodo, assicurati che i contenuti non siano stati diffusi.
Informa i/le ragazzi/e su ciò che dice la legge italiana sulla diffusione di materiale pedopornografico (L. 172/2012)
Se i contenuti sono online segnala ai servizi di Generazioni Connesse "clicca e segnala" o "stop it"
Coinvolgi la comunità scolastica nella sua interezza in percorsi di prevenzione dei comportamenti a rischio online
Coinvolgete la Polizia Postale e delle telecomunicazioni affinché rintraccino e blocchino i responsabili
Tieni traccia di quanto accaduto e delle azioni intraprese: compila il diario di bordo
Proponi la realizzazione di percorsi di sensibilizzazione e prevenzione dedicati a:
• Educazione all'affettività e alla sessualità (anche online)
• Immagine di sé online
• Relazioni online
Tieni traccia di quanto accaduto e delle azioni intraprese: compila il diario di bordo
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse al numero gratuito 1.96.96
MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
© All rights reserved Generazioni Connesse 2019


CO-FINANZIATO DALLA COMMISSIONE EUROPEA
Procedure interne: cosa fare in caso di Adescamento Online?
Generazioni Connesse
Studente/essa adescato/a online
Coinvolgi i genitori anche se chi coinvolto se ne vergogna ed è restio a farlo
Informa almeno una di queste figure:
• Il referente cyberbullismo;
• Il referente ePolicy;
• Il Dirigente Scolastico
Spiegagli/le che contenuti condivisi online possono rimanere o venire condivisi oltremodo
Coinvolgi la comunità scolastica nella sua interezza in percorsi di prevenzione dei comportamenti a rischio online
Parla della necessità di non divulgare i materiali online e dei pericoli connessi ad una diffusione incontrollata
Se i contenuti sono disponibili online segnala per rimuovere ai servizi di Generazioni Connesse "clicca e segnala" o "stop it".
Coinvolgete la Polizia Postale e delle telecomunicazioni affinché rintraccino e blocchino l'adescatore
Informa i ragazzi su ciò che dice la legge italiana sull'adescamento online (L. 172/2012)
Tieni traccia di quanto accaduto e delle azioni intraprese: compila il diario di bordo
Per qualsiasi dubbio, chiedi un consiglio telefonico alla helpline del progetto Generazioni Connesse Al numero gratuito 1.96.96
© All rights reserved Generazioni Connesse 2019

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



Elenco principali reati procedibili d'ufficio

Progetto regionale.
"Responsabili in classe e on-line"
www.responsabilionline-fvg.it

ISTITUTO COMPRENSIVO GEMONA DEL FRIULI

media educazione comunità

Scheda di approfondimento: I PRINCIPALI REATI PROCEDIBILI D'UFFICIO

Gli insegnanti, in quanto incaricati di pubblico servizio, hanno obbligo di denuncia qualora vengano a conoscenza di reati perseguibili d'ufficio. A questa categoria appartengono i seguenti reati:

Delitti "sessuali" (art. 609 bis e seguenti c.p.)

a) Violenza sessuale commessa nei confronti di minore di anni 18;
b) Violenza commessa dal genitore (anche adottivo) o dal di lui convivente, dal tutore o da persona alla quale il minore sia affidato per ragioni di cura, di educazione, di istruzione, di vigilanza o di custodia;
c) Violenza sessuale di gruppo;
d) Corruzione di minorenne (chi compie atti sessuali in presenza di un minore di 14 anni al fine di farlo assistere; chi fa assistere l'infra-quattordicenne ad atti sessuali o mostra materiale pornografico al fine di indurlo a compiere o subire atti sessuali);
e) Adescamento di minorenni (chi allo scopo di commettere reati di prostituzione minorile, pornografia minorile, detenzione di materiale pornografico, violenza sessuale, ...adesca un minore infra-sedicenne).

Prostituzione minorile* (600 bis)

Punisce chi recluta o induce alla prostituzione un minore di 18; favorisce, sfrutta, gestisce, ...la prostituzione di un minore di 18 anni; chi compie atti sessuali con un minore tra i 14 e i 18 anni in cambio di corrispettivo di denaro o altra utilità, anche solo promessi.

Pornografia minorile* (art. 600 ter) e Detenzione di materiale pedopornografico* (art. 600 quater c.p.)

Il presenti reati puniscono: chi utilizzando minori di anni diciotto realizza esibizioni o spettacoli pornografici ovvero produce materiale pornografico; chi recluta, induce minori di anni diciotto a partecipare a tali esibizioni o ne trae profitto; chi anche con il mezzo telematico, distribuisce, divulga, pubblicizza notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori di 18 anni; chi assiste a esibizioni o spettacoli pornografici in cui sono coinvolti minori di 18 anni; chi consapevolmente si procura, detiene, offre o cede ad altri, anche a titolo gratuito il materiale pornografico realizzato utilizzando minori di anni diciotto.

Minaccia* (art. 612 c.p)

Se qualcuno viene minacciato in modo grave (p.e. di morte) o con armi.

Lesione personale* (art. 582 c.p.)

Punisce chi procura lesione da cui deriva una malattia nel corpo o nella mente con prognosi superiore a 20 giorni o con circostanze aggravanti.

Stalking - atti persecutori* (art 612 –bis)

Chiunque, con condotte reiterate, minaccia o molesta un minore o una persona con disabilità (art.3 della legge 104/92) in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva, ovvero da costringere lo stesso ad alterare le proprie abitudini di vita.

Istigazione al suicidio* (art. 580 c.p.)

Chiunque determina altri al suicidio o rafforza l'altrui proposito di suicidio, ovvero ne agevola in qualsiasi modo l'esecuzione, è punito, se il suicidio avviene, con la reclusione da cinque a dodici anni. Se il suicidio non avviene, è punito con la reclusione da uno a cinque anni, sempre che dal tentativo di suicidio derivi una lesione personale grave o gravissima.

Estorsione* (art. 629 c.p.)

Punisce chi mediante violenza o minaccia costringe una persona a fare o omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno.

Violenza privata* (art. 610 c.p.)

Se una persona viene costretta con violenza o minaccia a fare, tollerare o omettere qualcosa (ad es. dover andare con qualcuno, ovvero non poter uscire ecc).

Sostituzione di persona* (art. 494 c.p.)

Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici.

Delitti contro l'assistenza famigliare (artt. 570 e seg. c.p.)

a) Violazione degli obblighi di assistenza famigliare se commessi nei confronti di minori
b) Abuso di mezzi di correzione o di disciplina;
c) Maltrattamenti in famiglia o verso i fanciulli.

***REATI ON-LINE:** la maggior parte dei reati sopra citati **possono essere commessi anche on-line** ovvero attraverso l'utilizzo di dispositivi connessi alla rete. Questa circostanza, che spesso rende più difficile l'individuazione del reato e più facile la sua attuazione da parte dei minori, può costituire in alcuni casi una aggravante del reato stesso.
Non ci sono tuttavia **reati specifici che descrivono questi comportamenti on-line e si deve quindi fare riferimento ai reati sopra elencati**. Ad esempio i comportamenti come il **Cyberbullismo** e il **Sexting** vanno valutati caso per caso in quanto possono includere uno o più dei reati perseguibili d'ufficio sopra elencati.

Informazioni in caso di necessità di un parere legale

-**Riferimento Nazionale: tel. 19696** - http://consulenzaonline.azzurro.it/xchatty/chat.html
(Telefono Azzurro – progetto Nazionale Generazioni Connesse)

-**Riferimento Regionale: tel. 0432.555708** Mail: garantefvg@regione.fvg.it
(Garante Regionale dei diritti alla persona del Friuli Venezia Giulia)

Fac-simile del *Modulo di prima segnalazione* (disponibile nella Bacheca del Registro elettronico)



MINISTERO DELL'ISTRUZIONE E DEL MERITO

ISTITUTO COMPRENSIVO STATALE

"F. BERNAGOZZI"

Scuola dell'Infanzia – Scuola Primaria – Scuola Secondaria di 1° grado
Piazza XX settembre, 17 - 44015 Portomaggiore – Tel. (0532) 811048
e-mail: feic824002@istruzione.it PEC: feic824002@pec.istruzione.it C.F. 93085160385

MODULO DI PRIMA SEGNALAZIONE (PRESUNTO) CASO DI BULLISMO

Tale modulo dovrà essere inviato alle docenti responsabili del Team Antibullismo, che provvederanno ad attivare il protocollo di segnalazione:
ilaria.mezzadri@icportomaggiore.org
letizia.parolini@icportomaggiore.org

Nome di chi compila la segnalazione ……

Plesso scolastico ……

1. La persona che ha segnalato il caso di presunto bullismo/cyberbullismo è

□ La vittima……..
□ Un compagno/a della vittima, nome……
□ Madre/padre/tutore della vittima nome……
□ Insegnante nome……
Altri……

2. Nome presunta vittima……
Classe:……
Altre presunte vittime:
Nome ……
Classe:……..
Nome ……
Classe:……..

3. Nome presunto bullo/a……
Classe:……
Altri presuntI bulli/e
Nome……
Classe:……
Nome……
Classe:……

4. Breve descrizione del problema o dell'accaduto:

- Che cosa è successo?……
□ Quando? ……
□ Dove? ……

- La vittima era da sola?
□ Sì
□ No Chi c'era? Segnalare nome e cognome ……

- La vittima ne ha parlato con qualcuno?
□ No
□ Sì Chi? Segnalare nome e cognome ……

- Quante volte sono successi gli episodi? ……

- Quando sono accaduti gli episodi? ……

5. Altre informazioni utili da segnalare:
……
……
……
……

Luogo ……

Data ……

Firma

……