

Documento di ePolicy

FGTD010004

A FRACCACRETA

VIA ADDA 2 - 71016 - SAN SEVERO - FOGGIA (FG)

Maria Soccorsa Colangelo

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

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

Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

Il documento di E-Policy ha lo scopo di informare tutta la comunità educante circa l'uso corretto e responsabile della rete e i rischi connessi a quest'ultima, in tutti i momenti che coinvolgono le attività didattiche. La E-Policy, inoltre, potrà costituire un supporto e fornire alcune linee guida per l'organizzazione dell'insegnamento di Cittadinanza digitale (Area 3 dell'insegnamento di Educazione civica).

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

Il Dirigente Scolastico, prof.ssa Maria Soccora Colangelo.

Le Referenti per il Contrasto al bullismo e cyberbullismo, prof.sse Anna Sessa e Rosanna Mazza.

L'Animatore Digitale: prof. ssa Giovanna Russo.

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.

Le principali figure coinvolte sono le seguenti, con i compiti evidenziati:

DIRIGENTE SCOLASTICO: oltre ad assicurare la sicurezza in rete di tutti gli appartenenti alla comunità scolastica, promuove attività di formazione dei docenti, degli studenti e del personale A.T.A.

ANIMATORE DIGITALE: affianca il Dirigente Scolastico nell'organizzazione e nella gestione delle attività di formazione, opera con il personale scolastico sia nelle operazioni tecniche di gestione della sicurezza informatica e di protezione dei dati sensibili, sia nell'opera di sensibilizzazione.

REFERENTI DEL BULLISMO E CYBERBULLISMO: si occupano di porre in essere azioni specifiche per il contrasto al bullismo e cyberbullismo, avvalendosi del supporto

di esperti interni o esterni alla scuola e delle forze dell'ordine, prestando particolare attenzione all'informazione e alla formazione della comunità scolastica.

I DOCENTI: hanno il compito di abituare gli studenti ad un uso responsabile delle TIC e della Rete. I docenti possono integrare nel curricolo sezioni volte alla riflessione, sensibilizzazione e formazione circa l'uso consapevole delle TIC e della Rete, secondo quanto previsto dall' insegnamento di "Educazione civica" (Area 3, "Cittadinanza digitale"); si ritiene inoltre opportuno usare le TIC e le risorse della rete a supporto della didattica. I docenti hanno inoltre il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso legato ad un impiego scorretto della Rete o delle TIC. Tale responsabilità diventa ancora più significativa in caso di attuazione della DaD e della DDI, come è accaduto durante l'emergenza Covid-19. In merito sono vigenti presso l'Istituto "A. Fraccacreta" sia un regolamento inerente alla Privacy, sia uno riguardante la DDI (si veda il dossier documenti presente nel sito istituzionale).

ATA: il personale ATA va coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo o cyberbullismo e deve operare in sinergia con le altre figure educative per raccogliere informazioni, verificare ed eventualmente segnalare al Dirigente Scolastico o al Referente del Cyberbullismo le criticità rilevate.

GLI STUDENTI E LE STUDENTESSE: dovrebbero usare in modo consapevole le TIC e imparare, con il supporto degli educatori, a tutelarsi in rete da qualsiasi pericolo possa loro presentarsi. Tale responsabilità è diventata ancora più significativa durante l'attuazione della DaD e della DDI. In merito è vigente presso l'istituto "A.Fraccacreta" sia un regolamento inerente alla Privacy, sia uno riguardante la DDI. E' altresì opportuno che gli studenti partecipino attivamente alle attività di formazione sul tema organizzate dalla scuola riguardanti i fenomeni di bullismo e cyberbullismo e il benessere digitale, facendosi anche promotori e promotrici di iniziative quali, ad esempio, la Peer education, compatibilmente con le condizioni sanitarie ammesse dall'emergenza Covid-19.

I GENITORI: dovrebbero agire in continuità con l'Istituto scolastico nella promozione ed educazione all'uso consapevole delle TIC e della rete, nonché all'uso responsabile dei device personali.

GLI ENTI EDUCATIVI ESTERNI E LE ASSOCIAZIONI: dovranno conformarsi alle procedure della scuola espresse attraverso il documento di e-policy e prendere visione dei regolamenti inerenti alla Privacy e alla DDI, applicandone i contenuti e segnalando eventuali comportamenti collegabili a bullismo o cyberbullismo. Vedasi: PNSD, L.n.107/2015.

1.3 - Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

L'istituto "A.Fraccacreta" ha definito un'informativa inerente alla privacy che dovrà essere rispettata da tutti i soggetti esterni che erogheranno attività educative all'istituto, sia in presenza sia eventualmente in modalità a distanza.

La modulistica di riferimento è visionabile nel sito della scuola al seguente indirizzo:

<https://www.itesfraccacreta.edu.it/index.php/pubblicitalegale/privacy>

1.4 - Condivisione e comunicazione dell'ePolicy all'intera comunità

scolastica

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

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

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

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

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

Nel corso di ogni anno scolastico, presso l'Istituto "A.Fraccacreta":

- agli studenti e alle famiglie sarà comunicata la presenza del documento e la sua funzione, tramite circolare sul registro elettronico. Inoltre sul sito della scuola sarà pubblicato per la consultazione l'intero documento dell'e Policy.
- alcuni docenti (individuati dal Dirigente scolastico) potranno dedicare parti delle loro lezioni a fornire indicazioni per un utilizzo sicuro del digitale, rinviando al documento di e-Policy;
- le famiglie saranno informate in merito alle procedure adottate dalla scuola per un uso sicuro e responsabile delle tecnologie digitali tramite la pubblicazione sul sito di istituto del presente documento, dei regolamenti e di tutte le iniziative attuate ai fini di una sua proficua applicazione (sia nella modalità in presenza sia eventualmente a distanza). L'informazione tramite il sito di istituto e tramite il Registro elettronico sarà la modalità prioritaria per comunicare alle famiglie le iniziative attuate dall'istituto.

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.

I docenti che eventualmente rilevino infrazioni ai regolamenti e alla E-Policy procederanno tramite richiamo verbale oppure tramite nota disciplinare sul registro elettronico, secondo l'entità della violazione;

l'infrazione verrà segnalata al Dirigente Scolastico che valuterà quale condotta adottare: convocazione dello studente, comunicazione alla famiglia o a chi ne fa le veci e, nei casi più gravi, segnalazione alla Polizia Postale, secondo quanto previsto dal Regolamento di Istituto, dal Patto di Corresponsabilità, dalla normativa inerente alla privacy;

eventuali provvedimenti disciplinari ritenuti necessari saranno adottati dal Consiglio di classe in accordo con il Dirigente Scolastico;

il Consiglio di classe, in accordo con la famiglia se lo studente è minorenni, potrà inoltre considerare l'eventualità di un supporto psicologico allo/la studente/ssa attraverso i servizi predisposti all'interno o all'esterno dell'istituto, qualora ciò fosse ritenuto necessario.

Eventuali infrazioni nell'uso del device o della Rete compiute dal personale scolastico saranno gestite dal Dirigente Scolastico, secondo quanto previsto dal Codice di comportamento dei dipendenti pubblici (GU n.129 del 4-6-2013), dal CCNL (29 novembre 2007), dal DPCM (28 novembre 2000) e dal Codice disciplinare pubblicato tramite il sito istituzionale e dalla normativa in vigore inerente alla privacy.

I documenti citati sono consultabili sul sito istituzionale.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

Il presente documento si integra inoltre per finalità e contenuti con il PTOF, con il Regolamento di Istituto, con quanto previsto dal Patto di Corresponsabilità, con i Regolamenti per l'utilizzo dei laboratori e della DDI, pubblicati sul sito istituzionale e con la documentazione inerente alla Privacy.

La documentazione citata è reperibile nel sito della scuola

(www.itesfraccacreta.edu.it)

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.

In particolare, presso il nostro istituto, a partire dall'entrata in vigore della presente E-Policy, le Referenti per il Bullismo e Cyberbullismo con il relativo gruppo di lavoro garantirà un monitoraggio della situazione dell'istituto. Inoltre l'Animatore Digitale, insieme al gruppo già citato, valuterà l'efficacia degli interventi e si considererà l'eventuale necessità di apportare modifiche alla e-Policy e ai regolamenti in vigore.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti (collegio docenti).

Azioni da svolgere nei prossimi 3 anni:

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



Capitolo 2 - Formazione e curriculum

2.1. Curriculum sulle competenze digitali per gli studenti

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

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

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

L'istituto "A.Fraccacreta" si propone di stilare nel corso del triennio un curriculum digitale di istituto, con il coinvolgimento del Dirigente Scolastico, delle Referenti per la Lotta al cyberbullismo, dell'Animatore Digitale, del TEAM Digitale, del Referente dell'Educazione civica: in particolare, secondo quanto previsto dalla normativa, ci si pone l'obiettivo di definire un curriculum verticale dell' Area 3 di Educazione civica ("Cittadinanza digitale"), valido come curriculum digitale. Per Cittadinanza digitale si intende la capacità di un individuo di avvalersi consapevolmente e responsabilmente dei mezzi di comunicazione virtuali.

Per consultazione, cliccare sul banner Educazione civica sul sito della scuola.

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 "A.Fraccacreta", che negli ultimi anni ha aderito e continua ad aderire al PNSD, anche utilizzando e valorizzando risorse interne adeguatamente formate, si propone di consolidare le competenze digitali del personale docente, anche attraverso momenti di formazione interna, da erogare in presenza o in modalità a distanza.

Nel corso dell' anno scolastico 2019-2020 si sono create le condizioni per l'aggiornamento dei docenti sulle TIC nella didattica, svolti nella prima parte dell'anno scolastico. Nella seconda parte dell'anno scolastico i docenti hanno curato il proprio aggiornamento attraverso corsi di formazione a distanza (webinar, videoconferenze), al fine di migliorare le competenze richieste dalla DaD e dalla DDI.

Per l' a. s. 2020 -21, i docenti hanno seguito un corso interno organizzato dall'Animatore Digitale. I docenti sono stati altresì informati di altre occasioni di aggiornamento (in particolare per quanto riguarda la Cittadinanza digitale, Area 3 di Educazione civica), tramite circolari pubblicate sul Registro elettronico.

Per l' a. s. 2021-22, sono stati effettuati degli incontri di formazione in presenza sull'utilizzo di piattaforme (Moodle). Inoltre la formazione ha previsto anche la conoscenza e l'utilizzo di Google drive, documenti e moduli Google, e cloud.

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.

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi on line. I Referenti per cyberbullismo si sono già formati sulla Piattaforma Elisa.

La formazione potrà essere arricchita anche tramite webinar appositi, soprattutto attivati da "GC" e "Telefono azzurro".

La formazione potrà prevedere anche qualche iniziativa promossa dall'istituto e potrà avvalersi dei numerosi corsi di aggiornamento a distanza riguardanti l'area 3 dell' Educazione civica. Ai docenti e al personale della scuola sarà consigliata anche nei prossimi anni un'adeguata formazione sull'utilizzo consapevole delle Tecnologie digitali e sulla normativa specifica.

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.

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC 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 ragazze verso un uso responsabile e consapevole delle tecnologie digitali. L'Istituto garantisce la massima informazione alle famiglie relativamente a queste tematiche, anche attraverso la conoscenza dell'ePolicy, del Regolamento d'Istituto e del Patto educativo di Corresponsabilità.

Sarà consigliata la consultazione del sito di "Generazioni Connesse" e di altri siti o piattaforme dedicate all'argomento. Data la situazione emergenziale, non si prevedono incontri in presenza rivolti alle famiglie, ma il sito di istituto diventerà un significativo veicolo di informazioni sul tema. La relativa sezione "Lotta al cyberbullismo" sarà aggiornata e potrà essere una fonte di informazioni per tutta la comunità scolastica.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.

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

Scegliere almeno 1 di queste azioni

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

In materia di PRIVACY il nostro Istituto ha messo in atto tutte le procedure necessarie per adempiere alla normativa in oggetto:

<https://www.itesfraccacreta.edu.it/index.php/pubblicitalegale/privacy>

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.

Nel nostro istituto, al fine di garantire l'effettivo diritto di accesso a Internet, ogni aula è dotata di un pc collegato alla rete e anche di una Lim.

Tutti i pc dei laboratori di Informatica (anche di Lingue, Matematica ed Economia aziendale) hanno connessioni a Internet e possono attingere al materiale condiviso tramite Server di istituto; inoltre, per scopi didattici gli studenti, solo con l'autorizzazione del docente, possono servirsi di device personali. Per motivi di sicurezza l'accesso ai predetti Laboratori è concesso agli studenti solo in presenza di un docente, assicurando inoltre che i comportamenti di tutti i presenti debbano essere consoni al Regolamento in vigore. Al fine di garantire agli studenti il diritto alla connessione e un uso didattico delle TIC, durante il periodo emergenziale della Dad sono stati consegnati in comodato d'uso alle famiglie vari PC portatili (previa autorizzazione del Dirigente Scolastico).

Al fine di garantire la sicurezza in rete, l'istituto si è dotato di un firewall, che fa capo ad una ditta esterna specializzata nel settore e che ha il controllo del firewall stesso. Il dispositivo, atto a garantire la sicurezza della rete, permette di monitorare il traffico in entrata e in uscita utilizzando una serie predefinita di regole per consentire o bloccare gli eventi su entrambe le reti dell’istituto. Sulla rete della didattica è applicato un controllo più restrittivo, riguardante sia la sicurezza e sia la tipologia di siti: risultano bloccati i siti pornografici. La rete della segreteria è sottoposta allo stesso controllo per quanto riguarda la sicurezza, così da garantire un monitoraggio sul traffico di dati in entrambe le direzioni, per impedire, sia in entrata che in uscita, connessioni pericolose per il sistema. In quest'ultimo caso non è applicato, però, alcun blocco sui siti visibili.

Si consiglia di consultare il documento Patto educativo di Corresponsabilità pubblicato sul sito della scuola.

3.3 - Strumenti di comunicazione online

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

Per il nostro istituto, durante l'anno scolastico 2019-20, è stato fondamentale il contributo delle tecnologie digitali al fine di garantire il diritto allo studio durante il periodo dell'emergenza Covid-19. L'esperienza e le competenze maturate da tutte le componenti della scuola sono state proficuamente impiegate e, all'occorrenza, implementate nel corso dell' a. s, 2020-21 al fine di applicare la DDi, secondo quanto previsto dal MIUR. Pertanto, in continuità con le linee applicate negli ultimi anni nell'ambito del PNSD, pur nel rispetto della libertà di docenza dei singoli docenti, l'istituto cercherà di proseguire una didattica che integri le metodologie della didattica "tradizionale" con l'impiego consapevole delle tecnologie digitali, tramite la valorizzazione della strumentazione a disposizione.

Strumenti di comunicazione fondamentali per l'utenza sono il sito istituzionale e il Registro elettronico. Fra gli strumenti di comunicazione esterna ricordiamo inoltre social network come Facebook e Instagram.

Invece fra gli strumenti di comunicazione con gli studenti (anche con i docenti) troviamo: mail istituzionale, piattaforma GSuite, classroom, Google Drive e piattaforma Moodle, per rendere più partecipata la didattica.

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.

Al momento l'utilizzo dei dispositivi personali all'interno dell' istituto viene regolato da quanto previsto nel Regolamento di Istituto, nel Regolamento della DDI, nell' informativa in materia di Privacy, da apposite circolari della DS inerenti ad aspetti specifici.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

- Organizzare attività volte a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity), nell'ambito dell'Educazione civica, area 3 Cittadinanza digitale.

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

Scegliere almeno 1 di queste azioni:

- Organizzare uno o più eventi o attività volti a informare e 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 informare e formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

In aggiunta agli interventi già previsti in tema di cittadinanza digitale, l'Istituto si impegna a svolgere un'attività di prevenzione e sensibilizzazione sulle seguenti tematiche:

Cyberbullismo
Hate speech
Dipendenza da Internet e gioco online
Sexting
Adescamento online
Pedopornografia .

A tal proposito saranno privilegiati (se possibile, data la situazione emergenziale) interventi esterni di esperti e/o associazioni che trattino le suddette tematiche e si cercherà di intensificare la collaborazione con le forze dell'ordine, impegnate nella prevenzione dei rischi e dei reati connessi all'uso improprio della rete, mediante incontri sia con gli studenti che con le loro famiglie.

Nell'attività di sensibilizzazione, già promossa da un nutrito gruppo di Peer educator, sono coinvolti anche i rappresentanti di Istituto, i quali avranno cura di proporre tali argomenti durante lo svolgimento delle Assemblee di Istituto, al fine coinvolgere tutta la vasta platea di studenti.

L'Istituto e i docenti si impegnano altresì a diffondere e promuovere tra gli studenti e le famiglie la conoscenza della piattaforma "Generazioni connesse" inserendo sul sito web istituzionale il link del progetto: www.generazioniconnesse.it, dove trovare ulteriori approfondimenti, spunti, aggiornamenti e strumenti didattici utili.

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).

Il nostro Istituto ha intenzione di:

- accrescere le capacità di intervento, sia in ottica preventiva, sia di gestione di eventuali episodi che si possono verificare;
- approfondire la conoscenza delle tecnologie digitali, del funzionamento del web, delle dinamiche dei social network;
- coinvolgere diversi attori, con particolare attenzione ai genitori e alle realtà aggregative territoriali, per garantire la promozione di azioni di prevenzione e contrasto, anche in contesti diversi da quello strettamente scolastico;
- interiorizzare e potenziare le competenze sociali e civiche;
- promuovere negli studenti comportamenti empatici e prosociali;
- promuovere negli studenti buone prassi comportamentali;
- promuovere la sicurezza in Rete degli studenti, perché acquisiscano le competenze necessarie all'esercizio di una cittadinanza digitale consapevole;
- supportare docenti e famiglie in momenti di difficoltà.

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.

Con Hate speech si indicano discorsi, azioni, contenuti e pratiche che esprimono intolleranza verso una persona o un gruppo di persone, identificate come appartenenti ad un gruppo o una categoria e che possono potenzialmente provocare reazioni violente a catena. Nella categoria “hate speech” rientrano dunque tutte le forme di espressione che incitano all’odio o alla violenza fondata su qualsiasi discriminazione (razziale, religiosa, di genere, di orientamento sessuale, etc).

La prevenzione dell’hate- speech è legata indissolubilmente all’educazione e alla sensibilizzazione alla diversità, da attuarsi all’interno della comunità educante attraverso azioni mirate alla conoscenza dell’altro e alla decostruzione degli stereotipi su cui si fonda l’hate-speech, nonché attraverso la promozione della partecipazione civica anche attraverso i media digitali e i social network.

4.4 - Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale?

La pervasività della tecnologia nella vita moderna, soprattutto per la generazione dei cosiddetti "nativi digitali" rende indispensabile la formazione all'uso corretto delle TIC, non solo in termini di educazione ai contenuti, ma anche di educazione ai tempi di utilizzo. Talvolta infatti, la tecnologia può indurre a quella che si definisce "dipendenza da internet", ossia un progressivo e totale assorbimento del soggetto alla rete. In caso di dipendenza, l'attività on line domina il soggetto assumendo un valore primario tra tutti gli interessi e riuscendo ad influire sulle alterazioni del tono dell'umore. Una delle declinazioni della dipendenza da internet è la NOMOFOBIA, ossia l'insieme di emozioni negative quali ansia, disagio e rabbia legati alla mancanza di connessione del soggetto col proprio smartphone. Troppo spesso il tempo trascorso in rete è impiegato nelle attività di gioco virtuale che in taluni casi può creare una vera e propria dipendenza (Net Gaming Addiction o Internet Gaming Addiction). Quella da gioco in rete presenta i sintomi di una vera e propria dipendenza quali un totale assorbimento al gioco, un'ossessione nei confronti dello stesso e il continuo impulso da parte del giocatore a giocare; impulso che, se non soddisfatto, porta a stati di agitazione, ansia o depressione.

Fondamentale è dunque che la scuola formi i ragazzi affinché l'uso della rete sia sempre sereno e consapevole, in modo da favorire il benessere digitale dei ragazzi stessi.

Qualora si riscontrino casi che coinvolgano gli studenti dell'Istituto, in accordo con le famiglie, saranno proposti eventuali percorsi educativi e/o di supporto psicologico ad opera di personale specializzato.

4.5 - Sexting

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

Il nostro istituto, nel rispetto della sensibilità degli studenti minorenni, ritiene opportuno informare gli alunni sull'argomento tramite l'incontro con esperti (ad esempio la Polizia postale), con eventuali iniziative di Peer education, che vedranno coinvolti alunni adeguatamente formati e personale specializzato, incentrate sul tema dell'educazione all'affettività e alla sessualità.

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.

E' sempre più frequente che le giovani generazioni facciano conoscenze e amicizie attraverso l'uso della Rete, con utilizzo di chat e social network. La mancanza di un contatto diretto con le persone conosciute comporta il rischio che gli amici virtuali siano in realtà persone male intenzionate, che adescano bambini o adolescenti su Internet allo scopo di intrecciare relazioni intime.

Il grooming è un fenomeno molto diffuso che non conosce distinzione di genere. I soggetti più esposti sono gli adolescenti, non solo perché vivono nella specifica fase della vita destinata alla costruzione di un'identità sessuale, ma anche a causa della curiosità insita all'adolescenza; ciò li porta a voler conoscere persone che possano iniziarli ad esperienze nuove.

Il grooming è particolarmente pericoloso perché l'adescatore cerca di intercettare i bisogni e i desideri dell'adolescente e manipolarli a proprio vantaggio, attraverso una dinamica non violenta ma instaurando un rapporto di fiducia con lo scopo di renderlo poi una relazione di tipo intimo.

La comunità educante ha dunque il compito di preparare gli studenti ai rischi nascosti in rete, attraverso incontri con esperti che trattino la tematica in un discorso più ampio di sicurezza e uso consapevole del web.

Qualora si riscontrino casi che coinvolgano gli studenti dell'Istituto, in accordo con le famiglie, saranno applicate le procedure previste dalla normativa vigente e proposti eventuali percorsi educativi e/o di supporto psicologico con esperti esterni.

La scuola quindi si impegna ad informare gli studenti e le studentesse circa la pericolosità di questo fenomeno, attraverso un uso consapevole e responsabile della rete. Infatti la nostra scuola intende promuovere percorsi di educazione (anche digitale) all'affettività e alla sessualità, anche con il supporto dei Peer Educator (educazione alla salute).

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](#).

Tenuto conto della delicatezza dell'argomento e, al contempo, della necessaria informazione ai fini preventivi e considerati gli evidenti legami con il fenomeno del sexting, l'istituto affronterà la tematica tenendo in considerazione la maturità, la fascia d'età e il tipo di informazioni che si possono condividere; inoltre, la trattazione sarà affidata a personale esperto (ad esempio la Polizia Postale). Al fine di informare e sensibilizzare tutta la comunità scolastica (genitori compresi) nei confronti della problematica, nell'apposita sezione (cliccare sul banner bullismo/cyberbullismo) del sito di istituto si potranno trovare utili informazioni.

Qualora si riscontrino casi che coinvolgano studenti dell'istituto, in accordo con le famiglie saranno applicate le procedure previste dalla normativa vigente, dal Regolamento di istituto, dal Patto di corresponsabilità e saranno proposti eventuali percorsi educativi o momenti di supporto psicologico ad opera di personale specializzato.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

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

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

Scegliere almeno 1 di queste azioni:

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/le studenti/studentesse, con il coinvolgimento di esperti.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di [Helpline 19696](#) e [Chat di Telefono Azzurro](#) per supporto ed emergenze;
- [Clicca e segnala di Telefono Azzurro](#) e [STOP-IT di Save the Children Italia](#) per

segnalare la presenza di materiale pedopornografico online.

Nell'affrontare i casi, la scuola prevede di instaurare rapporti di collaborazione con altre figure, enti e servizi presenti sul territorio, se la gravità e la sistematicità della situazione richiederà interventi che esulano dalle competenze e possibilità della scuola.

E' prevista la possibilità di seguire dei protocolli di collaborazione con dette istituzioni al fine di affrontare e risolvere nel migliore dei modi queste problematiche.

Tali procedure dovranno successivamente essere condivise con l'intera comunità educante, 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.

La condivisione di dette procedure può avvenire attraverso assemblee scolastiche, con l'utilizzo di materiale informativo da affiggere a scuola e durante i collegi 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](tel:19696).

Tra le possibilità sopra elencate l'istituto, secondo quanto indicato anche nel Regolamento di Istituto, in particolare si servirà di:

- due docenti Referenti per la lotta al bullismo e al cyberbullismo a cui comunicare le segnalazioni, prontamente riferite al Dirigente;
- un docente (1° Collaboratore) a cui comunicare le segnalazioni, prontamente riferite al Dirigente;
- un docente (Funzione Strumentale preposta) che si occuperà, all'occorrenza, di problemi collegati all'inclusione di ragazzi coinvolti in situazioni a rischio nella rete;
- uno sportello di ascolto o psicologico gestito da professionisti esterni all'istituto (a cui ricorrere nel caso in cui la procedura lo preveda);
- modulistica utile per la segnalazione, a disposizione degli studenti tramite il sito di istituto.

Si cercherà di portare a conoscenza degli studenti e delle studentesse il servizio Helpline del progetto Generazioni Connesse, contattabile tramite il numero gratuito [1.96.96](tel:19696).

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.

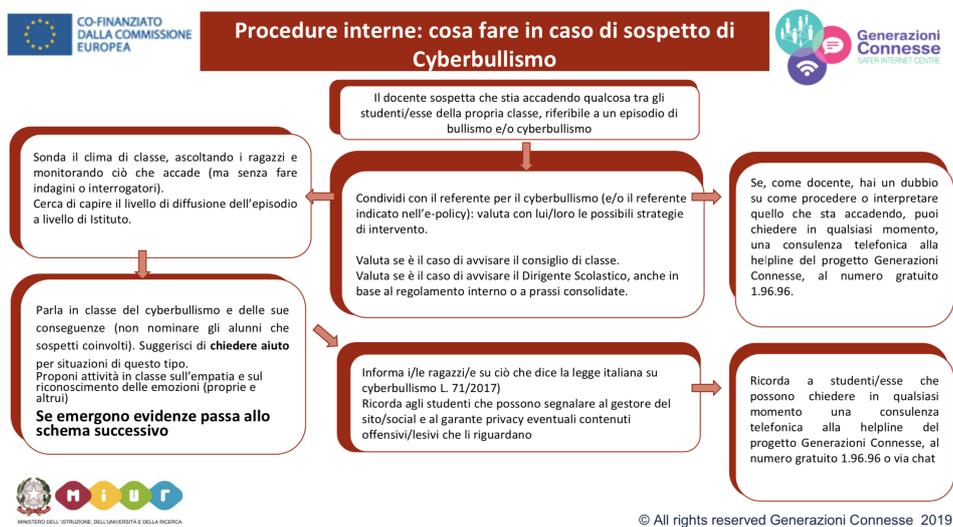
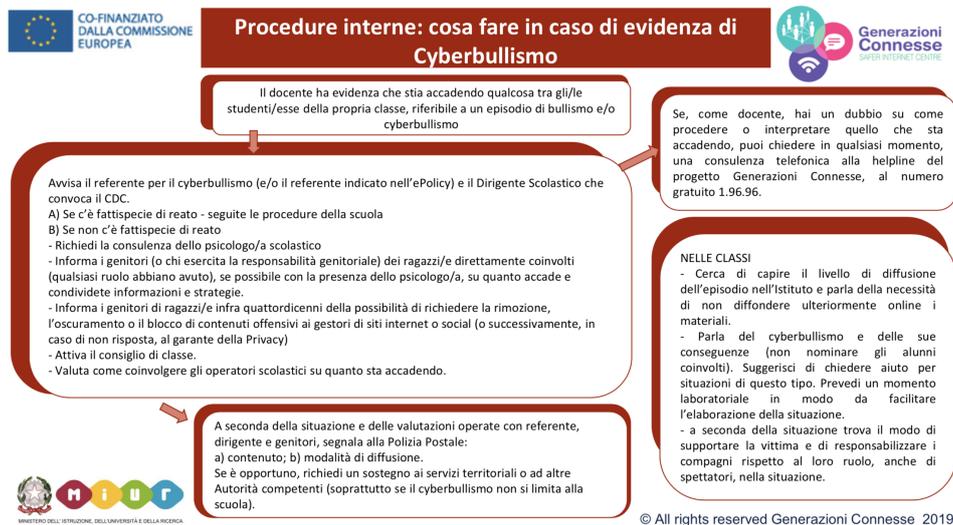
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all’utilizzo di Internet può presentare.

- **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.

Verranno individuate e contattate, in caso di necessità specifiche, eventuali associazioni e Istituzioni presenti sul territorio.

5.4. - Allegati con le procedure

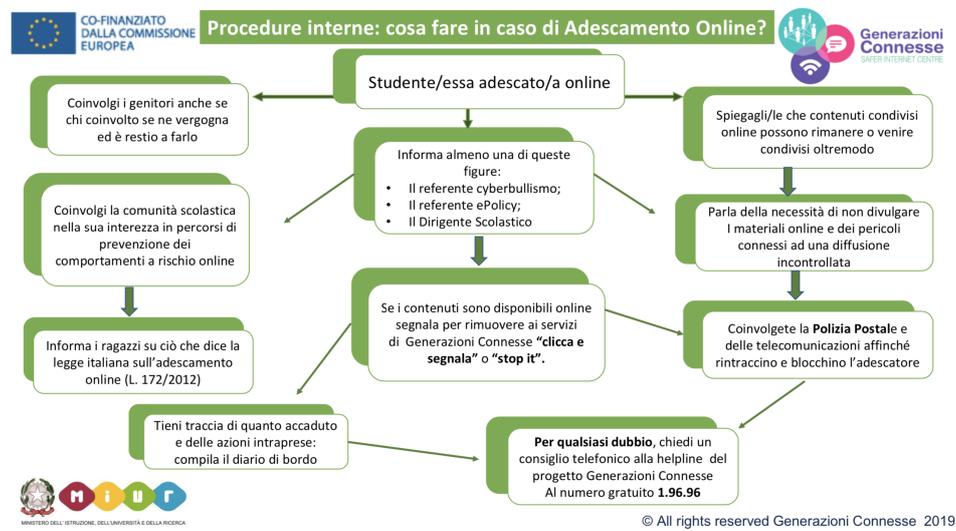
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



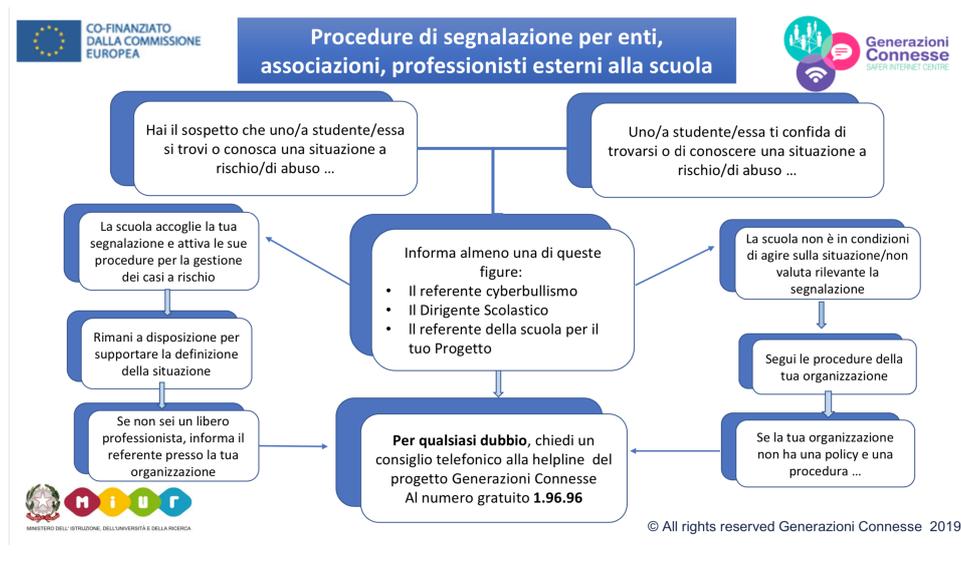
Procedure interne: cosa fare in caso di sexting?



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 Istituto, in caso di situazioni problematiche connesse all'uso delle tecnologie digitali, intende applicare le procedure sopra specificate. Sarà data di esse ampia informazione a tutti gli attori coinvolti, tramite il sito della scuola e il banner dedicato al bullismo/cyberbullismo.

Il nostro piano d'azioni

- Monitoraggio e perfezionamento delle procedure di segnalazione;
- Condivisione delle procedure con la comunità scolastica tramite il sito istituzionale, al fine di una migliore alleanza educativa tra scuola e famiglia;
- Promozione dell'Educazione al rispetto;
- Promozione dell'Educazione Civica Digitale.



