

Documento di ePolicy

FGIC82400L

I.C. "MONTI DAUNI"

LARGO S. NICOLA 2 - 71035 - CELENZA VALFORTORE - FOGGIA (FG)

Lorella Perniola

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.

Scopo del presente documento di e- policy è di informare l'utenza per un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente. In particolare l'intento della scuola è quello di promuovere l'uso consapevole e critico da parte degli alunni delle tecnologie digitali e di internet, di far acquisire loro procedure e competenze "tecniche" ma anche corrette norme comportamentali, di prevenire ovvero rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali .

Gli utenti, soprattutto minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto la Scuola promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti.

Gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose.

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.

Ogni utente connesso alla rete deve seguire le seguenti regole:

- rispettare il presente regolamento e la normativa vigente;
- tutelare la propria privacy, quella degli altri adulti e quella degli studenti;
- rispettare la "netiquette", galateo della rete.

Dirigente Scolastico

Il ruolo del Dirigente scolastico nel promuovere l'uso consentito delle tecnologie e di internet include i seguenti compiti: La responsabilità generale per i dati e la sicurezza dei dati; garantire che la scuola utilizzi un Internet Service filtrato approvato, conforme ai requisiti di legge vigenti; la responsabilità di assicurare che il personale riceva una formazione adeguata per svolgere i ruoli di sicurezza on-line e per la formazione di altri colleghi; essere a conoscenza delle procedure da seguire in caso di infrazione della EPolicy; ruolo di primo piano nello stabilire e rivedere la E-Policy; ricevere relazioni di monitoraggio periodiche della sicurezza online da parte del responsabile; garantire che vi sia un sistema in grado di monitorare il personale di supporto che svolge le procedure di sicurezza online interne.

Direttore dei Servizi Generali e Amministrativi

Il ruolo del direttore dei servizi generali e amministrativi include i seguenti compiti: assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni; garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore Digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.

Animatore digitale

Il ruolo dell'Animatore Digitale include i seguenti compiti:

- stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on-line e 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, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite password personali applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione);
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale"

Team digitale

Il ruolo del Team digitale include i seguenti compiti:

- pubblicare e diffondere la E-Safety Policy sul sito della scuola;

- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola;
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".

Docenti

I Docenti hanno la responsabilità di illustrare agli studenti il presente documento; dare indicazioni sul corretto uso della rete; supervisionare e guidare gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono la tecnologia on-line;

- Garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- Assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- Controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo all'Animatore Digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC
- segnalare al Dirigente Scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.

Alunni

Il ruolo degli alunni include i seguenti compiti:

- essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- avere una buona comprensione delle 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;

- comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

Genitori

Sostenere la scuola nel promuovere la sicurezza online e approvare l'accordo di E-Safety Policy con la scuola;

- partecipare agli incontri proposti dalla scuola relativamente alla sicurezza nell'uso di internet e delle tecnologie digitali e al cyberbullismo;
- non diffondere dati personali;
- adottare condotte rispettose degli altri quando si comunica in rete;
- conoscere le norme di utilizzo della rete nel rispetto del copyright e del diritto di autore;
- rispettare la normativa relativa alla privacy.

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

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

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

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

(numero, mail, chat, profili di social network).

Tutti gli altri operatori presenti a qualsiasi titolo nella scuola (esperti esterni, collaboratori, ditte esterne ...) dovranno attenersi alle norme previste per il personale scolastico.

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.

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.

- condivisione del documento nelle assemblee di classe;
 - incontri formativi.
-

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.

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali di internet di cui si dispone per la didattica, in relazione alla fascia di età considerate, sono prevedibilmente le seguenti:

- il collegamento a siti web non indicati dai docenti
- utilizzare la rete per interessi privati e personali che esulano dalla didattica
- scaricare file, video-musicali protetti da copyright deridere, offendere, insultare, calunniare attraverso l'uso delle TIC;
- minacciare attraverso l'uso delle TIC
- pubblicare sui social network o inviare tramite messaggistica immagini, video o testi che siano offensivi della dignità personale
- attuare cyberstalking o altre forme di persecuzione e molestia attraverso l'uso delle TIC

Sono previsti pertanto da parte dei docenti provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento, quali:

- il richiamo verbale
- il richiamo scritto con annotazione sul diario
- la convocazione dei genitori da parte degli insegnanti
- la convocazione dei genitori da parte del Dirigente scolastico
- La sospensione dalle lezioni

- La segnalazione agli assistenti sociali
- La segnalazione alle autorità competenti in caso di reati

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di prevenzione e gestione positiva dei conflitti, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni. L'infrazione della presente e-policy da parte del personale (docente, ATA,) può costituire elemento di contestazione d'addebito disciplinare e per gli esterni (esperti, collaboratori, etc.) può essere causa di risoluzione di eventuali contratti e/o convenzioni in essere.

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 con gli obiettivi e i contenuti dei seguenti documenti: PTOF e Regolamento d'Istituto. Il referente del bullismo/cyberbullismo con il suo gruppo di lavoro, in collaborazione con la Commissione PTOF, in raccordo con il Collegio Docenti, opera al fine di integrare i regolamenti dell'Istituto con il presente documento, apportandone le opportune modifiche da proporre al Consiglio d'Istituto.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il monitoraggio dell'implementazione della Policy e del suo eventuale aggiornamento sarà svolto ogni anno. Il monitoraggio sarà affidato al referente del bullismo/cyberbullismo e al suo gruppo di lavoro. L'aggiornamento della policy sarà curato dal Dirigente Scolastico, dal referente del bullismo/cyber bullismo e dal suo gruppo di lavoro, sulla base delle segnalazioni effettuate dal personale della scuola.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

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

Azioni da svolgere nei prossimi 3 anni:

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

Connesse rivolto agli studenti

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

Capitolo 2 - Formazione e 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.

Considerato che la competenza digitale è una delle competenze chiave per l'apprendimento permanente, identificata dall'Unione Europea, l'uso delle TIC per l'apprendimento è ormai indispensabile. "La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet" (Raccomandazione del Parlamento europeo relativa a competenze chiave per l'apprendimento permanente). Il curriculum della scuola del primo ciclo di istruzione sulle competenze digitali è trasversale alle discipline. Ciascuna classe sviluppa le competenze in un curriculum verticale flessibile, che tiene conto non solo dell'età degli alunni, ma anche dei prerequisiti che gli alunni già possiedono.

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.

Il nostro Istituto promuove l'utilizzo delle TIC nella didattica, a partire dalle prime aule computer, passando attraverso il piano di implementazione delle LIM. Di pari passo si sono succedute le attività di formazione informatica, alla formazione generalizzata per tutti i docenti per l'uso delle LIM, degli applicativi della G-Suite for Education, capillarmente diffuso nei nostri plessi, all'attuale percorso formativo relativo al Coding, che ha visto partecipazione massiccia. Il corpo docente è sensibile al tema del cyberbullismo e parteciperà a momenti formativi sul tema.

Nell'ambito del PNSD questa scuola

Ha individuato:

- La figura **dell'Animatore Digitale e un team digitale** con specifiche competenze nell'attuazione degli obiettivi e delle innovazioni previste dal PSND;
- La figura di referente per il cyberbullismo, con team d'emergenza e antibullismo con anche competenze in materia di sicurezza on-line.

Aderito a:

- Formazione interna guidata dall'Animatore Digitale, in particolare, allo sviluppo e alla diffusione del Pensiero Computazionale e del Coding.
-

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 formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica e la sicurezza in rete costituiscono una delle principali priorità della nostra scuola. Il nostro Istituto è particolarmente attento ad ogni iniziativa atta a raggiungere un buon livello di formazione in merito all'utilizzo e all'integrazione delle TIC nella didattica e alla sicurezza in rete. Tutti i docenti sono comunque sollecitati e prestare particolare attenzione all'auto formazione continua per rimanere sempre aggiornati in merito ad un mondo in continua evoluzione. L'Animatore Digitale promuove un incontro di Formazione dei docenti sul Progetto "Generazioni Connesse". Nell'arco di quest'anno i docenti seguiranno i corsi della piattaforma e incontri/seminari con esperti esterni e enti/associazioni, coinvolgendo anche studenti e genitori.

Sul sito della scuola verrà predisposto una sezione dal titolo: "Generazioni Connesse", a cui potranno accedere sia i docenti, che i genitori.

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.

La scuola darà ampia diffusione, tramite pubblicazione sul sito, del presente documento di policy per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e favorire un'attiva collaborazione tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi a un uso non consapevole e critico del digitale. Questo documento rappresenta il primo passo per sensibilizzare le famiglie dei nostri alunni affinché affrontino in modo consapevole i pericoli della rete stando a fianco dei docenti nelle loro attività didattiche basate sull'uso delle TIC. L'Istituto sta definendo un protocollo di incontri, tenuti da esperti o da docenti formati, da attuare annualmente per sensibilizzare le famiglie su cyberbullismo e sull'uso consapevole della rete e delle tecnologie digitali.

Il nostro piano d'azioni

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

- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

Il nostro piano d'azioni

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

- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

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 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 riferimento al dlgs 30 giugno 2003, n. 196 (c. d. Codice della Privacy) e al nuovo Regolamento europeo Privacy n. 679/2016, il nostro Istituto individua delle Linee Guida che disciplinano il trattamento dei dati personali gestiti:

- Predisposizione e condivisione con l'intera comunità scolastica di un'informativa che illustri il ruolo del DPO, la tipologia di dati raccolti, il loro utilizzo e il fine per cui vengono utilizzati;
- Predisposizione di apposito regolamento che disciplina l'uso di immagini e video;
- All'atto dell'iscrizione è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico di immagini e video;
- I nomi completi di alunne e alunni saranno evitati sul sito web come pure nei blog, forum e wiki, in particolare se in associazione con le loro fotografie;
- Predisposizione di una liberatoria specifica per la condivisione di immagini e video durante eventi a carattere pubblico particolarmente rilevanti;
- Predisposizione di una liberatoria specifica per la condivisione di elaborati ai fini della partecipazione a concorsi e a eventi pubblici;
- Predisposizione di liberatorie specifiche, contenenti le modalità di trattamento, la conservazione dei dati raccolti e le misure di sicurezza adottate per la somministrazione di questionari di ricerca e per la partecipazione ad attività che coinvolgono personale esterno alla scuola;
- Messa a disposizione dei genitori sul sito istituzionale del modello di reclamo al Garante per la protezione dei dati personali in caso di violazioni in materia di cyberbullismo; Regolamentazione sull'uso di dispositivi in grado di registrare e di strumenti compensativi previsti nei PDP/PEI.

Inoltre:

1. Creazione sul sito (www.isc-montidauni.edu.it) di due "Aree riservate", una per i Docenti e una per il Consiglio di Istituto alle quali si accede tramite password specifica;
2. Definizione, sul sito istituzionale della scuola, di una specifica sezione dedicata

- alla Privacy, evidente e raggiungibile con chiarezza dalla Home Page;
3. Pubblicazione, nella sezione Privacy, delle informative:
 - agli studenti e alle loro famiglie
 - al personale
 - ai fornitori
 - specifica per l'uso di G Suite (o altra piattaforma simile) per la attività didattiche a distanza e documentali.
 4. Pubblicazione, nella sezione Privacy, dei dati del DPO (nominativo, PEO, PEC, riferimento telefonico)
-

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.

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.

Secondo il Piano Nazionale Scuola Digitale (PNSD) , adottato con Decreto Ministeriale n. 851 del 27 ottobre 2015, la sfida dell’educazione nell’era digitale parte dall’accesso ad Internet.

Il PNSD prevede interventi specifici, promossi e coordinati dall’Animatore Digitale, in merito alla formazione degli insegnanti, al miglioramento delle dotazioni hardware, fino alle attività didattiche.

Per quanto riguarda la formazione l’animatore promuoverà la partecipazione a seminari, convegni, corsi on-line organizzati dagli Enti del territorio, dalle scuole in rete che partecipano al PNSD, da esperti interni e esterni alla Scuola.

Tali interventi saranno rivolti:

- ai docenti tutti e a quelli che avranno un profilo di accesso personale al sito, con il quale contribuiranno ad alimentare i contenuti didattici dello stesso;
- al personale amministrativo, dotato di un profilo di accesso personale al sito, che gestirà la comunicazione delle circolari, il registro elettronico e il personale;
- ai collaboratori scolastici, in primo piano nella comunicazione con gli utenti della scuola;
- alle famiglie, destinatarie di servizi on line.

Il processo avverrà in modo graduale.

Nel merito l’I.S.C. “Monti Dauni” è destinatario di due finanziamenti FSE-PON “Per la

scuola, competenze e ambienti per l'apprendimento" 2014-2020, Asse II:

- Avviso pubblico prot.n. 28966 del 6 settembre 2021 per la trasformazione digitale nella didattica e nell'organizzazione;
- Avviso pubblico prot.n. 20480 del 20/07/2021 per la realizzazione delle reti locali, cablate e wireless, nelle scuole.

Le attrezzature presenti nei laboratori e acquistate con precedenti finanziamenti pubblici sono in parte datate e non sempre fruibili dagli alunni. Sarebbe auspicabile una sostituzione con macchine più efficienti e nello specifico:

- Sostituzione delle Lim con Digital Board;
- Pc e monitor per il rinnovo dell'aula di informatica della scuola primaria e secondaria di 1° grado;
- Sistema antivirus per tutti i dispositivi dell'Istituto;
- Adeguamento delle infrastrutture tecnologiche e multimediali (per uffici e didattica) per favorire la dematerializzazione, conservazione sostitutiva e digitalizzazione.

L'Istituto ha bisogno di strumentazioni, di attrezzature specifiche, di dispositivi che facilitino l'innovazione della didattica quali:

- Tablet per la creazione di spazi alternativi per l'apprendimento;
- Strumenti compensativi per DSA: smart Pen, audiolibro o libro parlato, sintesi vocali, correttore ortografico vocale, registratori di testi cartacei+scanner+OCR, software per costruzione di mappe e schemi;
- scanner professionale;
- stampante 3D;
- software specifici;

L'Istituto attualmente, grazie alla partecipazione precedenti bandi PON è dotato:

- di un cablaggio in parte wireless e in parte LAN. Con i nuovi finanziamenti si provvederà a migliorare e rendere più efficienti le reti, ad aggiornare le infrastrutture in modo da avere una rete adeguata al numero degli studenti e in grado di supportare il traffico di dati generato da un numero elevato di studenti.
- di device (tablet, chromebook e notebook) da dare in comodato d'uso gratuito agli alunni nel caso di DAD ed eventualmente ai docenti.

Essendo l'I.S.C. "Monti Dauni" articolato su più plessi, la password per l'accesso a Internet è diversa per ogni plesso. Ciascun utente connesso alla rete dovrà: rispettare il presente regolamento e la legislazione vigente succitata, tutelare la propria privacy, quella degli altri utenti adulti e degli alunni al fine di non divulgare notizie private

contenute nelle documentazioni elettroniche cui ha accesso.

I genitori saranno invitati a firmare e restituire un modulo di consenso.

Al fine di garantire la safety nell'accesso ad Internet gli studenti saranno guidati allo sviluppo di competenze digitali per un uso consapevole delle TIC e della RETE e al rispetto della "netiquette" (insieme di regole, comunemente accettate e seguite da quanti utilizzano Internet e i servizi di rete, che disciplinano il comportamento di un utente nel rapportarsi agli altri utenti attraverso risorse come wiki, newsgroup, mailing list, forum, blog o e-mail).

L'Istituto si propone di dotarsi di una PUA (Politica uso accettabile e sicurezza della rete): norme di buon utilizzo che la scuola si impegna a redigere e a divulgare prima che sia concesso l'accesso a Internet alla componente studentesca.

La security sarà invece implementata attraverso l'adozione delle seguenti misure cautelative:

- Mantenere separate le reti didattica e segreteria: importante per garantire maggiore sicurezza alle informazioni, gestendo in modo autonomo e con regole differenti le due reti grazie al firewall;
- Aggiornare periodicamente software e Sistema operativo: garantire che il sistema sia aggiornato lo protegge dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo;
- Definire la programmazione di backup periodici: cioè la copia e messa in sicurezza dei dati del sistema scolastico per prevenire la perdita degli stessi (possibilmente anche una copia offline);
- Definire la programmazione di backup periodici: cioè la copia e messa in sicurezza dei dati del sistema scolastico per prevenire la perdita degli stessi (possibilmente anche una copia offline).
- Garantire formazione adeguata allo staff, incluso il corpo docenti: la formazione deve riguardare la gestione dei dispositivi, la conoscenza delle regole basilari sulla sicurezza. Testare regolarmente le possibili vulnerabilità;
- Preparare piani di azione in risposta ai problemi più seri: è importante non dover improvvisare nel momento in cui si verifica un problema serio, ma avere un protocollo di azione;
- Predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo: se non è previsto uno stand-by, il dispositivo resta accessibile nel caso in cui qualcuno dimentichi di spegnerlo, con il rischio potenziale di accesso da parte di persone non autorizzate;
- Impostare il browser per l'eliminazione dei cookies alla chiusura: in questo modo si evita che qualcuno possa avere accesso ad account altrui senza autorizzazione;
- Definire una policy sulle password;

- Sviluppare il regolamento sull'uso delle tecnologie a scuola (policy di uso accettabile): deve riguardare chiunque abbia accesso alla Rete, studenti/esse, docenti, amministrazione e segreteria, includere i dispositivi della scuola e quelli personali, anche in caso di BYOD;
 - Adottare sistemi di filtraggio software e hardware o servizi specifici forniti da Internet provider per bloccare contenuti dannosi o materiali non adatti
-

3.3 - Strumenti di comunicazione online

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

La nostra DS coordina la comunicazione interna ed esterna del nostro Istituto a partire da un piano di comunicazione in grado di trasmettere all'esterno l'identità, i valori, le azioni, i progetti e l'idea di educazione che la scuola porta avanti. Sono stati individuati i docenti responsabili del Sito Web e della pagina FB di Istituto. Sia la pagina Facebook che il sito web dell'I.S.C. "Monti Dauni" rispondono a specifici regolamenti approvati dal Consiglio di Istituto.

Altri mezzi di comunicazione online in dotazione alla scuola sono: il registro elettronico con tutte le sue funzionalità, lo sportello di segreteria digitale e la sua bacheca istituzionale.

Inoltre, l'I.S.C. "Monti Dauni" utilizza il dominio riservato Google Workspace (ex G Suite) per:

- la comunicazione e collaborazione interna. Attraverso l'account a dominio è possibile l'accesso in cloud a tutta una serie di applicazioni, tra cui Google Drive, Meet, Gmail, Chat e Hangouts che, nel loro insieme, costituiscono il sottosistema informatico per la comunicazione e la collaborazione;
- la DDI, tramite Meet, Classroom, Calendar, Google Drive e gli altri applicativi della Suite di Google.

Agli studenti e a tutto il personale della scuola è stato assegnato un account GSuite per il dominio dell'Istituto: nome.cognome@isc-monbtidauni.edu.it.

Alle famiglie è stata inviata l'informativa riguardo all'uso e alle caratteristiche di

Google Workspace (ex G Suite for Education)

Per la messaggistica istantanea testuale o in videocall (docenti-docenti e docenti-genitori) si utilizzeranno Chat e Hangouts di Google Workspace, evitando di utilizzare whatsapp, così come esplicitamente indicato dalle direttive europee.

Sia per la DDI che per le riunioni in modalità telematica sono stati predisposti specifici regolamenti approvati dagli organi collegiali competenti.

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

1. andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari);
2. risultati scolastici (voti, documenti di valutazione);
3. udienze (prenotazioni colloqui individuali);
4. eventi (agenda eventi);
5. comunicazione varie (comunicazioni di classe, comunicazioni personali).

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

Il riepilogo delle medie con relative valutazioni ed eventuali assenze è accessibile sul registro elettronico AXIOS dal profilo dei Coordinatori di classe.

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.

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/le 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.

L'I.S.C. "Monti Dauni" dispone il divieto dell'utilizzo del cellulare o di altri dispositivi elettronici per uso personale. È consentito il loro utilizzo previa autorizzazione scritta dei docenti indicante data e ora. Tale divieto è codificato nel Regolamento d'Istituto (Art. n. 63, comma4). La violazione di tale divieto configura un'infrazione disciplinare rispetto alla quale la scuola è tenuta ad applicare apposite sanzioni.

Sia alunni (quando autorizzati dal docente) e i docenti sono tenuti a spegnere i propri cellulari prima dell'ingresso in aula.

Per implementare la dotazione scolastica relativa alle TIC e favorire il BYOD il nostro Istituto si impegna a redigere una PUA che regolamenti l'uso dei dispositivi personali.

Il nostro piano d'azioni

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

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

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

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- 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 i genitori 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.

La necessità di sensibilizzare gli studenti ad un utilizzo sicuro e consapevole delle tecnologie digitali, sia in un'ottica di tutela dai rischi potenziali che di valorizzazione delle opportunità esistenti, pone tutta la comunità educante di fronte alla sfida di riconsiderare la propria identità, le proprie risorse e il proprio ruolo educativo.

Il nostro Istituto intende perseguire:

- **azioni di sensibilizzazione**, rivolte al personale docente e Ata, agli studenti/studentesse e ai genitori, mediante la collaborazione con i servizi territoriali locali (Forze di Polizia, ASL, Cooperative, Associazioni...);
 - **azioni di prevenzione**, rivolte agli studenti/studentesse, al fine di formare e consolidare quelle competenze educative di base necessarie a poter gestire le situazioni di vita che i ragazzi sperimentano online.
-

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 cyberbullismo presenta una serie di caratteristiche specifiche:

- **L'impatto:** la diffusione di materiale tramite Internet è incontrollabile e non è possibile prevederne i limiti (anche se la situazione migliora, video e immagini potrebbero restare online e continuare a diffondersi). Un contenuto offensivo e denigratorio online può, quindi, diventare virale e distruggere in alcuni casi la reputazione della vittima. Nelle situazioni più gravi, le vittime di cyberbullismo si trovano costrette a dover cambiare scuola o addirittura città, ma questo spesso non le aiuta. La Rete, si sa, è ovunque.
- **La convinzione dell'anonimato:** chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile. Sentendosi protetti dall'anonimato ci si sente liberi e più forti nel compiere atti denigratori, senza il timore di essere scoperti. È importante tenere bene a mente, però, che quello dell'anonimato è un "falso mito della Rete". Ogni nostra azione online è, infatti, rintracciabile e riconducibile a noi con gli strumenti opportuni o con l'intervento della Polizia Postale. L'anonimato del cyberbullo, inoltre, è anche uno dei fattori che stanno alla base del forte stress percepito dalla vittima, la quale molte volte non può dare né un nome e né un volto al proprio aggressore.
- **L'assenza di confini spaziali:** il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo dei suoi spazi-rifugio. La vittima può essere raggiungibile anche a casa e vive nella costante percezione di non avere vie di fuga. Spegnerne il cellulare o il computer non basta, così come cancellare tutti i propri profili social. Il solo pensiero che eventuali contenuti denigratori continuino a diffondersi online è doloroso e si accompagna ad un senso costante di rabbia e impotenza.
- **L'assenza di limiti temporali:** può avvenire a ogni ora del giorno e della notte.
- **Il feedback non tangibile:** il cyberbullo non vede in modo diretto le reazioni della vittima e, ancora una volta, ciò riduce fortemente l'empatia e il riconoscimento del danno provocato.
- **L'indebolimento dell'empatia:** esistono cellule chiamate neuroni specchio che ci permettono di "leggere" gli altri quando li abbiamo di fronte, capirli e di provare emozioni simili a quelle che loro provano, proprio come se fossimo di fronte ad uno specchio. Tale sensazione è data dall'attivazione di una particolare area del cervello. Quando le interazioni avvengono prevalentemente

online la funzione speciale di questi neuroni viene meno (mancando la presenza fondamentale dell'altro che è sostituito dal dispositivo). La riduzione di empatia che ne consegue può degenerare nei comportamenti noti messi in atto dai cyberbulli.

È possibile suddividere gli atti di cyberbullismo in due grandi gruppi:

- **cyberbullismo diretto:** il bullo utilizza strumenti di messaggistica istantanea (es. sms, mms) che hanno un effetto immediato sulla vittima, poiché diretti esclusivamente a lei;
- **cyberbullismo indiretto:** il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima anche da un punto di vista psicologico.

È molto importante sottolineare come il cyberbullismo non sia una problematica che riguarda unicamente vittima e cyberbullo. È un fenomeno sociale e di gruppo. Infatti, centrale è il ruolo delle agenzie educative e di socializzazione (formali e informali) più importanti per gli adolescenti: la famiglia, la scuola, i media, le tecnologie digitali e il gruppo dei pari. In ottemperanza a quanto previsto dalla Legge 71/2017 recante "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" e relative Linee guida di aggiornamento 2021, il nostro Istituto ha individuato un Referente per la prevenzione ed il contrasto del bullismo e cyberbullismo, affiancato da un Team operativo d'emergenza e antibullismo. È stato stilato e successivamente aggiornato un Protocollo di prevenzione e contrasto al bullismo e al cyberbullismo.

Di seguito si riportano le azioni di prevenzione che il nostro Istituto intende intraprendere:

- prevedere percorsi formativi per gli insegnanti in merito al fenomeno del bullismo e del cyberbullismo;
- promuovere il benessere a scuola attraverso percorsi di alfabetizzazione emotiva;
- prevedere progetti di "educazione digitale" per gli studenti, al fine di migliorare le loro competenze digitali e sensibilizzare circa i possibili pericoli presenti in Rete, anche mediante il coinvolgimento di partners esterni alla scuola (Polizia postale, Associazioni...);
- promuovere un ruolo attivo degli studenti in attività di peer education;
- regolamentare l'uso del web, attraverso filtri che non consentano l'accesso a siti rischiosi o contenenti materiale non adatto ai ragazzi e il monitoraggio del tempo di esposizione alle nuove tecnologie, affinché risulti quantitativamente e qualitativamente adeguato;
- integrare il Regolamento d'Istituto e il Patto Educativo di Corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti.

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.

- Prevedere progettualità socio-educative, che valorizzino la dimensione emotiva e relazionale degli studenti e potenzino le loro capacità di analisi e discernimento.
- Prevedere momenti formativi per la promozione del rispetto della diversità, al fine di combattere ogni forma di discriminazione (razziale, etnica, religiosa, di genere, di orientamento sessuale, di disabilità).
- Educare ad un uso etico e consapevole delle tecnologie.
- Educare alla legalità ed alla convivenza civile.

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?

Negli ultimi anni si registra un aumento del "popolo dei navigatori quotidiani" che coinvolge ogni fascia di età. Infatti, grazie alla Rete, i bambini trovano nuove opportunità di gioco, i giovani e gli adulti si informano, comunicano, commerciano e sperimentano se stessi attraverso la cosiddetta comunicazione virtuale. Ma, come tutti gli strumenti di comunicazione, anche la Rete non è esente da cattivi usi e da abusi che portano ad una moderna forma di dipendenza, definita internet-dipendenza. Il bilanciamento tra opportunità e rischi negli ambienti mediali e in relazione ai più giovani, richiede una costante e attenta negoziazione tra opportunità e rischi. Internet dovrebbe avere un utilizzo "integrativo", incentivando e accompagnando le attività dei ragazzi nel mondo reale: divertirsi con gli amici, coltivare hobby, fare sport... Quando la Rete assume, invece, un ruolo "sostitutivo", è un problema su cui bisogna intervenire. Si evidenzia, quindi, come la dipendenza da Internet, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica che deve attenzionare il fenomeno e fornire gli strumenti agli studenti e alle studentesse affinché questi siano consapevoli dei rischi che comporta l'iperconnessione. La scuola può insegnare molto da questo punto di vista se integra la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online.

Il nostro Istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale che prevedono:

- un piano di "educazione digitale" che promuova l'uso consapevole e responsabile degli strumenti digitali;
- l'adozione di una linea condivisa con le famiglie, per stabilire mezzi e modalità durante lo studio domestico, con tempi definiti e controllo attivo durante la navigazione in Rete.

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 medialmente 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.

I contenuti sessualmente espliciti possono diventare materiale di ricatto assumendo la forma di "revenge porn" letteralmente "vendetta porno" fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte (la Legge 19 luglio 2019 n. 69, all'articolo 10 ha introdotto in Italia il reato di revenge porn, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti).

Tra le caratteristiche del fenomeno vi sono principalmente:

- **La fiducia tradita:** chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo, inoltre, alla motivazione della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale).
- **La pervasività con cui si diffondono i contenuti:** in pochi istanti e attraverso una condivisione che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso a un numero esponenziale e infinito di persone e ad altrettante piattaforme differenti. Il contenuto, così, diventa facilmente modificabile, scaricabile e condivisibile e la sua trasmissione è incontrollabile.
- **La persistenza del fenomeno:** il materiale pubblicato online può permanere per un tempo illimitato e potrebbe non essere mai definitivamente rimosso. Un contenuto ricevuto, infatti, può essere salvato, a sua volta re-inoltrato oppure condiviso su piattaforme diverse da quelle originarie e/o in epoche successive.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/i e depressione. La prima prevenzione al sexting avviene in famiglia e trova le sue basi nella trasmissione forte dei valori familiari, educando al rispetto verso sé stessi e verso gli altri. La scuola, poi, è il contesto educativo in cui il ragazzo trascorre la maggior parte del suo tempo. Parlare in famiglia e a scuola del rispetto che occorre avere verso sé stessi, significa portarli a ragionare sul concetto di autostima, aiutandoli a sviluppare un pensiero critico per imparare a "saper dire di no", di fronte a richieste che potrebbero metterli in imbarazzo. Oltre al rispetto, è importante promuovere il concetto di empatia, facendo in modo che i ragazzi si rendano conto che vi è un'altra realtà al di fuori della propria e invitandoli, quando necessario, a mettersi nei panni degli altri.

Le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica prevedono:

- percorsi di formazione rivolti ai docenti, agli studenti/studentesse e ai genitori, per approfondire i rischi e le conseguenze di episodi di sexting;
 - incontri laboratoriali finalizzati ad approfondire aspetti importanti, quali la consapevolezza del proprio valore e della propria immagine, l'importanza di agire quanto prima, parlandone con una figura adulta, i temi del rispetto e della responsabilità, le forme sanzionatorie e di tutela.
-

4.6 - Adescamento online

Il **grooming** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di **teen dating** (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies - l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

Potenziali vittime dell'adescamento online possono essere sia bambini che bambine, sia ragazzi che ragazze. Il fenomeno, infatti, non conosce distinzione di genere. Gli adolescenti sono particolarmente vulnerabili, poiché si trovano in una fase della loro vita in cui è molto importante il processo di costruzione dell'identità sessuale. L'adescamento non avviene apparentemente con una dinamica violenta, ma il "prendersi cura" del minore rappresenta la conditio per carpirne la fiducia ed instaurare una relazione a sfondo erotico. Per riconoscere un eventuale caso di adescamento online è importante prestare attenzione a piccoli segnali (ad esempio il possesso di conoscenze sessuali non adeguate all'età), che possono essere indicatori importanti, per valutare un cambiamento improvviso nel comportamento di un minore.

Per prevenire ed affrontare la delicata problematica dell'adescamento il nostro Istituto

intende promuovere:

- percorsi di Educazione all'affettività e alla sessualità, anche in collaborazione con gli esperti, al fine di aiutare i ragazzi a gestire le proprie emozioni, l'immagine di sé, il rapporto con il proprio corpo e con gli altri;
- l'attivazione di un servizio di supporto psicologico (Sportello di Ascolto), al fine di fornire un valido aiuto agli studenti e alle studentesse in difficoltà.

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](#).

La pedopornografia esiste da prima dell'avvento di Internet. Tuttavia, la diffusione della Rete, l'evoluzione e la moltiplicazione dei "luoghi" virtuali, il cambiamento costante delle stesse tecnologie digitali, ha radicalmente cambiato il modo in cui il materiale pedopornografico viene prodotto e diffuso, contribuendo ad un aumento della sua disponibilità e dei canali di diffusione. Qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, questo per facilitare il processo di rimozione del materiale stesso dalla Rete e allo stesso tempo consentire le opportune attività investigative finalizzate ad identificare chi possiede quel materiale, chi lo diffonde e chi lo produce, ma, soprattutto, ad identificare i minori abusati presenti nelle immagini e video, assicurando la fine di un abuso che potrebbe essere ancora in corso e il supporto necessario. Parallelamente, se si ravvisa un rischio per il benessere psicofisico delle persone minorenni coinvolte nella visione di questi contenuti, sarà opportuno rivolgersi ad un servizio deputato ad offrire un supporto psicologico anche passando per una consultazione presso il medico di base o pediatra di riferimento. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza (Consultori Familiari, Servizi di Neuropsichiatria infantile, centri specializzati sull'abuso e il maltrattamento all'infanzia, etc.). Se si è a conoscenza di tale tipologia di reato, è possibile far riferimento alla: Polizia di Stato - Compartimento di Polizia postale e delle Comunicazioni; Polizia di Stato - Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri - Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato - Commissariato online.

Le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica prevedono:

- incontri di sensibilizzazione rivolti ai docenti, agli studenti/studentesse e ai genitori, per promuovere la conoscenza del fenomeno;
- la promozione del servizio Hotline di Generazioni Connesse per le segnalazioni;
- l'attivazione di un servizio di supporto psicologico (Sportello di Ascolto), al fine di fornire un valido aiuto agli studenti e alle studentesse in difficoltà.

Il nostro piano d'azioni

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

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/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.

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

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

studenti/studentesse.

Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le 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'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/le 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.

Il nostro Istituto ha previsto un protocollo d'azione nel caso in cui si verificano atti che si configurano come Bullismo, Cyberbullismo, Sexting e Adescamento online.

Cosa segnalare:

- **contenuti afferenti alla privacy e non autorizzati (foto o video personali, l'indirizzo di casa o il telefono, informazioni private proprie o di altri, ecc.);**
- **contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto e video imbarazzanti, virus, contenuti razzisti o inneggianti al suicidio, immagini o video umilianti, insulti, ecc.);**
- **contenuti afferenti alla sessualità (messaggi molesti, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, ecc.)**

5.2. - Come segnalare: quali strumenti e a chi

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

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

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

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

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

Strumenti a disposizione di studenti/esse

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

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

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito [1.96.96](tel:19696).

Chi segnala:

Il docente, il Consiglio di classe, il Referente bullismo e cyberbullismo e il Dirigente Scolastico.

Nello specifico, 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.

Come segnalare:

Sul sito nel nostro Istituto, nella sezione appositamente dedicata al contrasto al bullismo e cyberbullismo (<http://www.isc-montidauni.edu.it>), sono a disposizione di docenti, alunni e famiglie diversi materiali e strumenti approvati in sede collegiale:

- **modello prima segnalazione dei casi di presunto bullismo e vittimizzazione;**
- **valutazione approfondita dei casi di bullismo e vittimizzazione;**
- **modello per segnalare episodi di bullismo sul web o sui social network e chiedere l'intervento del Garante per la protezione dei dati personali;**
- **scheda di monitoraggio.**

La prima segnalazione sarà presa in carico dall'insegnante che rileva il presunto caso di bullismo e cyberbullismo e riferirà al Referente. Quest'ultimo, assieme con il Team di emergenza, valuterà la situazione e, qualora il comportamento

segnalato rappresenti un vero e proprio illecito, informerà immediatamente il DS che convocherà le famiglie degli alunni interessati per gli adempimenti del caso, a seconda del livello di gravità.

Gli studenti hanno inoltre la possibilità di usufruire della consulenza dello psicologo dello **Sportello d'ascolto** se abilitato annualmente presso il nostro Istituto e/o utilizzare in tempo reale **l'App YouPol** realizzata dalla Polizia di Stato.

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.

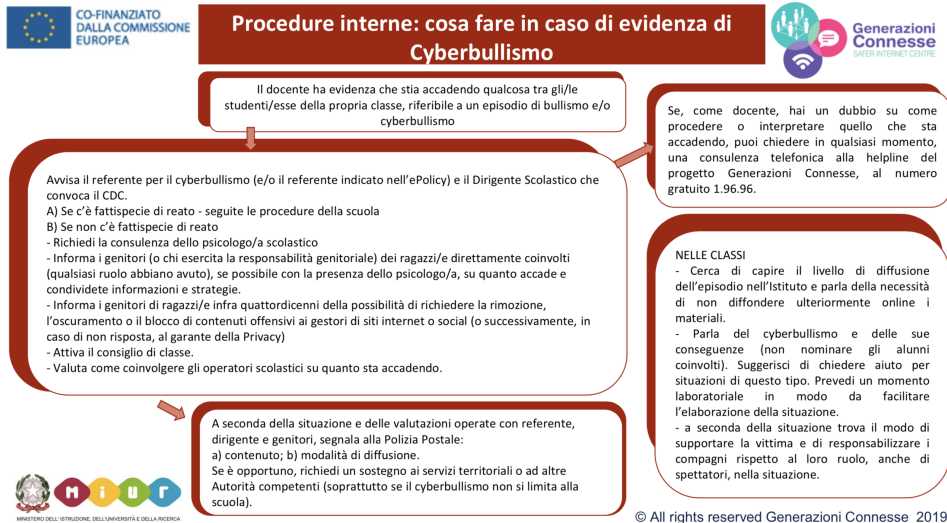
Nella gestione di alcuni casi, soprattutto in quelli valutati come Codice rosso, è indispensabile fare ricorso ad altri attori che si trovano sul Territorio della Regione Puglia:

- **ASL provinciale;**
- **Co.re.com;**
- **Ufficio Scolastico Regionale;**
- **Tribunale per i minori;**
- **Polizia Postale;**
- **Garante Regionale per l'Infanzia e l'Adolescenza.**

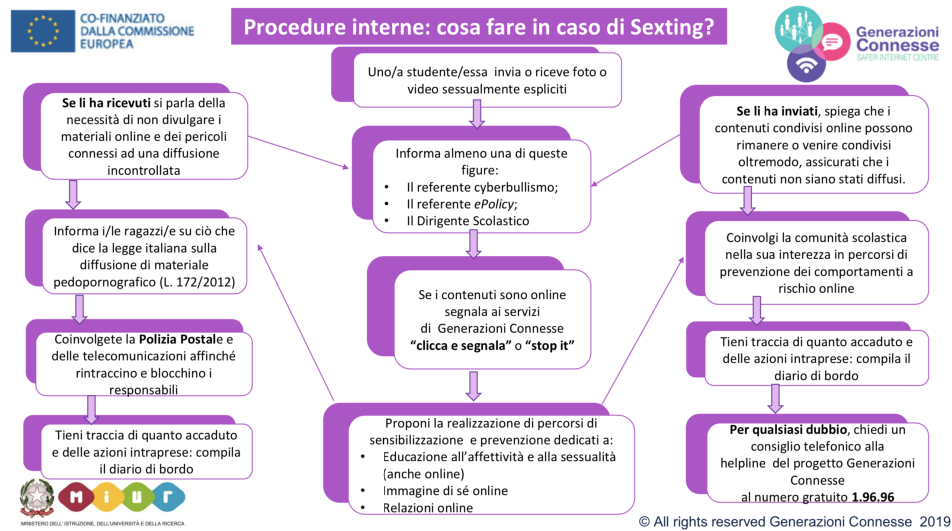
Il nostro Istituto intende avviare un Protocollo d'Intesa quale rete di scopo, con la Polizia Postale di Foggia. Quest'ultima offre la propria consulenza in materia di Bullismo, Cyberbullismo, Sexting e Grooming, nonché momenti formativi rivolti ai docenti, agli studenti e alle famiglie con lo scopo di sensibilizzare ad una condotta civile ed informarli sulle conseguenze giuridiche, sulla sicurezza informatica, gestione della Privacy e sulle procedure da attivare.

5.4. - Allegati con le procedure

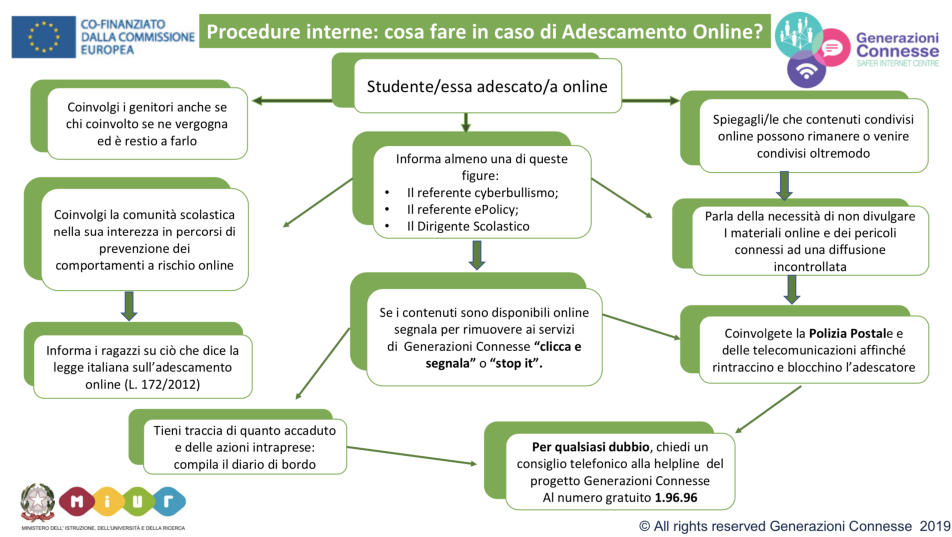
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



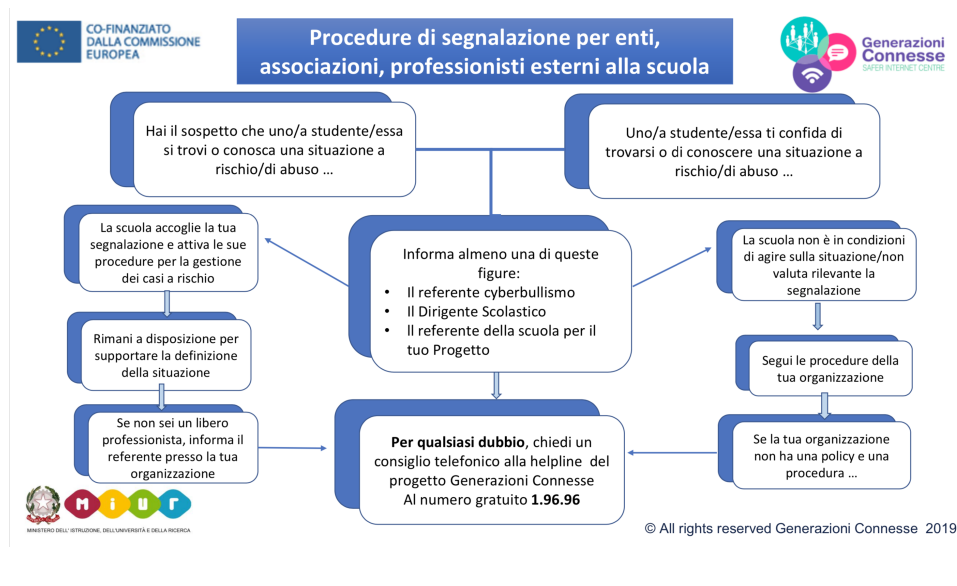
Procedure interne: cosa fare in caso di sexting?



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](#)

Procedure scolastiche in caso di atti di Bullismo e Cyber-bullismo

1ª Fase: analisi e valutazione dei fatti

Soggetto responsabile: Dirigente Scolastico e Docenti del Consiglio di Classe

Altri soggetti coinvolti: Referente, Gruppo operativo sul Bullismo e Cyberbullismo/Psicologo della Scuola/Team per l'emergenza.

- Raccolta di informazioni sull'accaduto: quando è successo, dove, con quali modalità.
- Interviste e colloqui agli attori principali, ai singoli, al gruppo; vengono raccolte le diverse versioni e ricostruiti i fatti ed i punti di vista. In questa fase è importante astenersi dal formulare giudizi; è piuttosto necessario creare un clima di empatia, di solidarietà e di disponibilità al confronto che permetta un'oggettiva raccolta di informazioni; l'adulto è un mediatore in un contesto neutro.

L'Istituto mette a disposizione le schede di prima segnalazione, sia per il bullismo che per il cyberbullismo, e un modello per chiedere l'intervento del Garante per la

protezione dei dati personali circa il bullismo sul web.

2ª Fase: risultati sui fatti oggetto di indagine

Soggetto responsabile: Dirigente Scolastico, Referente Bullismo e Docenti del Consiglio di Classe

Altri soggetti coinvolti: Gruppo operativo Cyberbullismo/Team per l'emergenza/Psicologo della Scuola.

I fatti sono confermati, esistono prove oggettive e quindi si apre un protocollo e vengono stabilite le azioni da intraprendere. L'Istituto mette a disposizione la scheda di valutazione approfondita per i casi di bullismo e vittimizzazione.

3ª Fase: azioni e provvedimenti

Se i fatti sono confermati:

- Comunicazione alla famiglia della vittima da parte del Dirigente Scolastico/Docente Coordinatore (convocazione scritta o telefonica) e supporto di tutto il Consiglio di classe nell'affrontare la situazione segnalata, concordando modalità di soluzione e analizzando le risorse disponibili dentro e fuori della scuola (psicologo, ASL, Enti Territoriali); in questa fase è importante evitare che la vittima si senta responsabile.
- Comunicazione ai genitori del bullo/cyberbullo (convocazione) con lettera del Dirigente; il D.S. valuterà che non ci sia rischio di inquinamento delle prove.
- Convocazione del Consiglio di Classe e valutazione del tipo di intervento disciplinare, secondo la gravità: sospensione del diritto a partecipare ad attività complementari ed extrascolastiche; sospensione attiva a scuola con svolgimento di attività rieducative; imposizione al bullo/cyberbullo di svolgimento di azioni positive (per es. lettera di scuse a vittima e famiglia); eventuale avvio della procedura giudiziaria per indagini: denuncia ad un organo di polizia o all'autorità giudiziaria (questura, carabinieri, ecc.) per attivare un procedimento penale (solo per soggetti da 14 anni in su). Nel caso la famiglia non collabori, giustifichi, mostri atteggiamenti oppositivi o comunque inadeguatezza, debolezza educativa o sia recidiva nei comportamenti: segnalazione ai Servizi Sociali del Comune.
- Valutazione di un intervento personalizzato →obiettivi: sviluppo dell'empatia, dell'autocontrollo, aumento della positività, evidenza delle conseguenze di ogni comportamento, sviluppo delle abilità di dialogo, di comunicazione e di negoziazione.

4ª Fase: percorso educativo e monitoraggio

Il Dirigente, il Referente, i Docenti di classe e gli altri soggetti coinvolti:

- si occupano del rafforzamento del percorso educativo all'interno della classe

e/o del gruppo coinvolti;

- provvedono al monitoraggio del fenomeno e della valutazione dell'intervento attuato sia nei confronti del cyberbullo, sia nei confronti della vittima.

L'Istituto mette a disposizione la scheda di monitoraggio il cui scopo generale è quello di valutare l'eventuale cambiamento a seguito dell'intervento/degli interventi (es. sono terminati i comportamenti di bullismo messi in atto verso la vittima) e se tale miglioramento della situazione rimanga stabile nel tempo (es. non si ripresentino prese in giro dopo qualche settimana quando l'attenzione sul caso potrà sembrare diminuita). In particolare, si dovrebbero prevedere almeno due momenti: a breve termine, entro una settimana; a lungo termine dopo circa un mese.

Il nostro piano d'azioni

Attività e iniziative messe in atto dall'"IC Monti Dauni"

In seguito alla Legge 29 maggio 2017 n. 71 recante "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", le successive Linee guida del MIUR (ottobre 2017), e il relativo Aggiornamento 2021 con nota prot. 482 del 18.02.2021, la Scuola ha ritenuto opportuno istituire un Team antibullismo composto da alcuni docenti dell'Istituto e un Team operativo per la gestione delle segnalazioni e delle emergenze su questa tematica. Nel corso degli anni l'Istituto ha dimostrato notevole impegno in materia, attivando iniziative formative tese a stimolare il senso di appartenenza al gruppo e a promuovere la libera espressione individuale, sviluppando il senso morale e di responsabilità anche al fine di ridurre potenziali situazioni di prevaricazione e prepotenza.

Di seguito vengono riportati i percorsi da noi attivati e ascrivibili alla sfera di prevenzione del bullismo e cyberbullismo; è stato inoltre creato uno spazio apposito sul sito per una puntuale informazione sulla materia e sulle iniziative avviate, i livelli d'intervento per l'anno scolastico in corso e futuri.

LIVELLO DI INTERVENTO	ATTORI COINVOLTI	OBIETTIVI	ESEMPI DI ATTIVITÀ
Comunità/ Territori	<ul style="list-style-type: none"> • UST • ASL • USR • GDPR (responsabile incaricato) • Tribunale dei Minori • Servizi sociali • Istituzioni pubbliche • Forze dell'ordine • Associazioni e gruppi ecc. 	<ul style="list-style-type: none"> • Sensibilizzare e coinvolgere la comunità territoriale; • Beneficiare delle risorse presenti sul territorio; • Costruire alleanze educative trasversali tra gli ambienti di vita dei nostri alunni. 	<ul style="list-style-type: none"> • Stesura di protocolli di intesa con gli Enti locali e le Forze dell'ordine, a seconda della gravità del caso; • Predisposizione di accordi con Enti, associazioni, servizi; • Coinvolgimento della comunità in serate di "in-formazione".
Scuola	<ul style="list-style-type: none"> • Personale scolastico (Staff) • Alunni • Genitori 	<ul style="list-style-type: none"> • Sensibilizzare sul problema del bullismo e del cyberbullismo; • Coinvolgere tutte le componenti, responsabilizzandole; • Proporre specifiche attività per promuovere il benessere a scuola e anti-bullismo; • Promuovere strategie per un uso consapevole di internet e delle tecnologie digitali, tramite anche la stesura del documento di e-policy. 	<ul style="list-style-type: none"> • Creazione di Team (antibullismo/emergenze), adeguatamente formati, la cui formazione acquisita ricadrà a cascata su altri docenti con appositi seminari tenuti a scuola dal Referente o Referenti nominati (possibilmente con competenze psico-pedagogiche); • Raccolta di dati sulla eventuale presenza nella scuola del fenomeno e analisi delle sue caratteristiche (modelli di segnalazione in allegato); • Formulazione di una politica scolastica e di un sistema di regole anti-bullismo; • Direttive sull'utilizzo delle nuove tecnologie a scuola; • Incontri di formazione per genitori; • Monitoraggio costante da parte dei docenti a scuola; • Eventuale partecipazione al progetto "Generazioni Connesse" (coordinato dal MIUR) o ad altri progetti.

Classe	<ul style="list-style-type: none"> • Alunni • Insegnanti 	<ul style="list-style-type: none"> • Creare un clima sereno e aperto al dialogo; • Favorire la cooperazione e la soluzione pacifica dei conflitti; • Aumentare il grado di consapevolezza sul problema; • Conoscere le regole basilari della comunicazione e del comportamento sul Web (concetti di Privacy e responsabilità); • Acquisire gli strumenti per gestire le situazioni problematiche (sia nelle relazioni sociali face to face che virtuali). 	<ul style="list-style-type: none"> • Attività di alfabetizzazione alle emozioni; • Percorsi di educazione alla legalità e alla convivenza civile; • Attività curriculari specifiche sul bullismo e cyber (film e video, letture, discussioni, laboratori di teatro, ecc.); • Percorsi atti a favorire conoscenza e utilizzo dei nuovi media; • Interventi specifici, anche di esperti, sui rischi in rete e sui comportamenti corretti da mettere in atto.
Singolo individuo	<ul style="list-style-type: none"> • Soggetti coinvolti 	<ul style="list-style-type: none"> • Saper fornire aiuto e sostegno adeguati sia alle vittime che ai bulli, perché riescano a scardinare il loro ruolo, costruendone uno coerente con la propria società. 	<ul style="list-style-type: none"> • Colloqui con gli alunni e le famiglie. • Interventi coordinati del gruppo operativo, insegnanti, alunni, famiglie coinvolte ed eventuali esperti esterni.

