Documento di ePolicy

RAIC824004

I.C. "S.P. DAMIANO" RAVENNA

VIALE LUIGI CILLA 8 - 48123 - RAVENNA - RAVENNA (RA)

Maria Guiati

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

1.2 - Ruoli e responsabilità

Affinché l'E-policy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, s'impegni nell'attuazione e promozione di essa.

Il Dirigente Scolastico:

- garantisce la tutela degli aspetti legali riguardanti la privacy;
- garantisce la sicurezza on-line dei membri della comunità scolastica;
- attiva le procedure previste in caso di violazione del regolamento nell'utilizzo delle TIC a scuola.

L'Animatore digitale (con il Team Digitale):

- stimola la formazione di competenze relative alla "scuola digitale" e fornisce consulenza in merito alla conoscenza, prevenzione e gestione dei rischi on-line;
- propone la diffusione di pratiche innovative o migliorative e i conseguenti aggiornamenti dei regolamenti dell'Istituto
- coinvolge la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti alla "scuola digitale".

Il Referente del bullismo e cyberbullismo e il Team:

- promuovono iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo,
- promuovono e gestiscono l'applicazione del protocollo interno per la gestione dei casi di bullismo e cyberbullismo
- coinvolgono (ove possibile), con progetti e percorsi formativi, studenti, colleghi e genitori.

Il referente per le nuove tecnologie:

- assicura, supportato dal tecnico informatico esterno, una corretta manutenzione delle attrezzature informatiche e una corretta protezione delle stesse da attacchi malevoli esterni;

L'amministratore di Google WorkSpace for education:

- amministra secondo le indicazioni fornite dal DS, la piattaforma Google WorkSpace for education, registrata con il dominio damiano.istruzioneer.it;
- assegna ad ogni membro del personale scolastico un account per l'accesso e l'utilizzo della piattaforma a fini didattici, lavorativi e organizzativi;
- assegna a tutti gli alunni autorizzati dai genitori o da chi ne ha la tutela legale un account per l'accesso e l'utilizzo didattico, nei modi e limiti definiti dal Ds, della piattaforma valido fino alla conclusione del primo ciclo di istruzione, salvo revoca della suddetta autorizzazione;
- aggiorna gli account degli utenti ed elimina gli account non più validi;
- produce annualmente le nuove rubriche degli utenti e le condivide con tutto il personale dell'Istituto.

Il Direttore dei servizi generali e amministrativi:

- assicura, 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;
- garantisce il funzionamento dei diversi canali di comunicazione della scuola (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.

Personale A.T.A. (Amministrativi):

- rispetta la presente ePolicy;
- utilizza, in modo professionale, i canali ufficiali della scuola per le comunicazioni digitali con gli studenti e le loro famiglie;
- assicura la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- segnala problemi o formula proposte al DSGA, per l'elaborazione di soluzioni e innovazioni sul piano dell'utilizzo e della sicurezza delle Tic.

Personale A.T.A. (collaboratori scolastici):

- rispetta la presente ePolicy;
- esegue la pulizia di PC, laptop, cavi e proiettori cercando di non muoverli e senza utilizzare supporti umidi o bagnati per evitare danni di carattere elettrico;
- assicura la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- segnala problemi relativi all'utilizzo improprio delle Tic da parte degli alunni.

I Docenti:

- rispettano la presente ePolicy;

- si informano sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di Internet e sulla politica di sicurezza adottata dalla scuola;
- diffondono tra gli alunni le modalità per utilizzare le TIC in modo sicuro e corretto;
- sensibilizzano gli alunni riguardo le potenzialità del Web in quanto strumento di ricerca, da utilizzarsi nel rispetto della normativa sui diritti d'autore;
- utilizzano, in modo professionale, il canale ufficiale della scuola per le comunicazioni digitali con gli studenti e le loro famiglie;
- assicurano la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllano l'uso delle tecnologie digitali e dei dispositivi mobili da parte degli alunni durante le lezioni, i cambi d'ora e ogni altra attività scolastica (ove consentito);
- nelle lezioni in cui è programmato l'utilizzo di Internet, verificano che gli alunni accedano con le proprie credenziali e li guidano a siti adatti all'attività prevista;
- comunicano ai genitori le eventuali problematiche emerse nel caso di un utilizzo non appropriato delle TIC da parte dei propri figli,
- segnalano problemi o formulano proposte all'Animatore Digitale e al referente per le nuove tecnologie, per l'elaborazione di soluzioni e innovazioni sul piano dell'utilizzo e della sicurezza delle Tic;
- si assumono la responsabilità di non divulgare le credenziali di accesso agli account e/o alla rete wifi
- prima di lasciare la postazione di lavoro effettuano correttamente il logout

Gli Alunni:

- rispettano la presente ePolicy;
- utilizzano le TIC a scuola solo su indicazioni del docente
- accedono all'ambiente di lavoro con l'account personale del quale non divulgano le credenziali di accesso
- in caso di riscontro di malfunzionamenti della strumentazione e/o di contatto accidentale con informazioni, immagini e/o applicazioni inappropriate lo comunicano immediatamente all'insegnante
- non utilizzano la strumentazione della scuola a scopi personali, ludici e/o ricreativi (a meno che l'attività didattica non lo preveda esplicitamente)
- non utilizzano dispositivi personali senza aver avuto il permesso da parte dell'insegnante
- chiudono correttamente la propria sessione di lavoro prima di lasciare la postazione
- Rispettano quanto riportato nel regolamento di disciplina (scuola secondaria): 1. Lo studente deve tenere sempre il cellulare spento durante il periodo di permanenza a scuola (compreso l'intervallo) e in tutti i contesti didattici fuori dalla scuola (palestra, uscite didattiche di qualsiasi tipo). Il telefono deve essere spento prima dell'ingresso a scuola e può essere riacceso solo all'uscita.

La comunicazione con le famiglie, per qualsiasi urgenza, è sempre garantita attraverso il telefono della scuola. Nel caso in cui le linee telefoniche della scuola siano inagibili o momentaneamente inattive, per motivi di servizio, il docente in servizio può autorizzare l'uso del dispositivo. Il divieto d'uso del cellulare a scuola risponde ad una esigenza prettamente educativa, tesa a favorire la socializzazione e le relazioni dirette tra le persone. 2. L'uso di PC o tablet qualificati come strumenti compensativi per alunni con bisogni educativi speciali sarà consentito solo secondo le modalità concordate dai docenti con l'alunno e la famiglia e regolarmente indicate nel PDP o PEI dell'alunno. 3. L'uso di PC o tablet o altre tipologie di devices per attività didattiche in cui ne sia previsto l'uso sarà regolato puntualmente dal docente che organizza questa attività e gli alunni dovranno attenersi rigorosamente alle indicazioni fornite nelle consegne di lavoro. 4. E' vietato riprendere immagini o compiere registrazioni audio e video con qualsiasi apparecchiatura all'interno dell'edificio scolastico senza autorizzazione. Le infrazioni saranno punite con sanzioni disciplinari severe e, se ritenuto opportuno, potranno essere denunciate alle autorità competenti per le conseguenze previste dalla vigente normativa. Tale divieto è esteso anche alle visite guidate ed ai viaggi di istruzione. 5. Si ribadisce il divieto di utilizzare il cellulare durante l'orario di servizio per il personale docente e non docente della scuola. L'utilizzo di dispositivi elettronici personali (tablet, PC, ...) è consentito ai docenti solo per finalità didattiche (firma e compilazione del registro elettronico, utilizzo di applicazioni didattiche, ...).

- Rispettano quanto riportato nell'integrazione del Patto di Corresponsabilità educativa introdotta nel 2020 in seguito all'introduzione della DAD: • Conservare la password personale e non consentirne l'uso ad altre persone. • Comunicare immediatamente all'amministrazione di sistema l'impossibilità ad accedere al proprio account o il sospetto che altri possano accedervi. • Non consentire ad altri, a nessun titolo, l'utilizzo della piattaforma Google WorkSpace for Education. • Non diffondere eventuali informazioni riservate di cui venisse a conoscenza, relative all'attività delle altre persone che utilizzano il servizio. • Utilizzare i servizi offerti solo ad uso esclusivo per le attività didattiche della scuola. • Assumersi la piena responsabilità di tutti i dati inoltrati, creati e gestiti attraverso la piattaforma Google WorkSpace for Education. • Rispettare gli orari di svolgimento delle lezioni. • Indossare un abbigliamento adeguato.
- Rispettano la NETIQUETTE riportata all'interno dell'intergazione al Patto di corresonsabilità: • Quando ci si avvale di un computer in modo non esclusivo, utilizzare sempre il browser Google Chrome in modalità OSPITE, non memorizzare la password ed effettuare sempre il logout; • In POSTA e in GRUPPI inviare messaggi brevi che descrivano in modo chiaro l'oggetto della comunicazione; indicare sempre chiaramente l'oggetto in modo tale che il destinatario possa immediatamente individuare l'argomento della mail ricevuta; • Non inviare mai lettere o comunicazioni a catena (es. catena di S. Antonio o

altri sistemi di carattere "piramidale") che causano un inutile aumento del traffico in rete; • Non utilizzare la piattaforma in modo da danneggiare, molestare o insultare altre persone; non creare e non trasmettere immagini, dati o materiali offensivi, osceni o indecenti; • Non creare e non trasmettere materiale offensivo per altre persone o enti. Non creare e non trasmettere materiale commerciale o pubblicitario; • Quando si condividono documenti non interferire, danneggiare o distruggere il lavoro dei docenti o dei compagni; • Non violare la riservatezza degli altri studenti; • Usare il computer e la piattaforma Google SWorkSpace in modo da mostrare considerazione e rispetto per compagni e insegnanti.

I Genitori:

- rispettano la presente ePolicy;
- contribuiscono, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- sostengono i figli nel rispettare i regolamenti scolastici per l'utilizzo delle TIC, le indicazioni per l'accesso a Internet e l'utilizzo sicuro dello stesso, il regolamento interno di Istituto e il patto di corresponsabilità in conformità con quanto richiesto dai docenti;
- agiscono in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite.

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).

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

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

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

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

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

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

1.5 - Gestione delle infrazioni alla ePolicy

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

I provvedimenti disciplinari hanno finalità educativa, tendono al rafforzamento del senso di responsabilità e al ripristino di rapporti corretti all'interno della comunità scolastica. Le sanzioni sono sempre temporanee, devono essere ispirati al principio della responsabilizzazione personale, proporzionate all'infrazione disciplinare ed ispirate al principio di gradualità nonché, per quanto possibile, al principio della riparazione del danno. Esse tengono conto della situazione personale dello studente, della gravità del comportamento e delle conseguenze che da esso derivano. Allo studente è sempre offerta la possibilità di convertirle in attività a favore della comunità scolastica (DPR 249 / 98 art. 4 punto 5 così come modificato dal DPR 235/2007). Agli alunni che manchino ai loro doveri scolastici sono inflitte, secondo la gravità della infrazione, le seguenti sanzioni disciplinari:

a) Rimprovero verbale.

b) Consegna da svolgere in classe.

c) Consegna da svolgere a casa.

d) Invito alla riflessione guidata sotto l'assistenza di un docente.

e) Ammonizione scritta con annotazione sul registro elettronico (eventualmente anche sul diario) e comunicazione immediata alla famiglia;

f) Nota disciplinare sul registro elettronico;

g) Esclusione dalla partecipazione ai viaggi di istruzione, uscite didattiche, attività sportive straordinarie (tornei, competizioni, ecc.), attività ludiche, con obbligo di presenza a scuola;

h) Sospensione scolastica con obbligo di frequenza a scuola;

i) Temporaneo allontanamento dalla comunità scolastica fino ad un massimo di 15 giorni in caso di gravi o reiterate infrazioni disciplinari (D.P.R. 249/98 art.4 punto 7 così come modificato dal DPR 235/2007).

j) Allontanamento dalla comunità scolastica per un periodo superiore ai 15 giorni quando siano stati commessi reati che violano la dignità e il rispetto della persona umana o vi sia pericolo per l'incolumità delle persone. In tale caso, in deroga al limite generale previsto dall'art. 4 punto 7 del D.P.R. 249/98 così come modificato dal DPR 235/2007, la durata dell'allontanamento è commisurata alla gravità del reato ovvero al permanere della situazione di pericolo. Si applica, per quanto possibile, il disposto dell'art. 4 punto 8 del DPR 235/2007 (DPR 249/98 art. 4 punto 9 così come modificato dal DPR 235/2007).

k)Allontanamento dalla comunità scolastica per tutto l'anno scolastico con l'esclusione

dallo scrutinio finale o la non ammissione all'esame di Stato conclusivo del corso di studi o, nei casi meno gravi, dal solo allontanamento fino al termine dell'anno scolastico; ciò nei casi di recidiva, di atti di violenza grave, o comunque connotati da una particolare gravità tale da ingenerare un elevato allarme sociale, ove non siano esperibili interventi per un reinserimento responsabile e tempestivo dello studente nella comunità durante l'anno scolastico. (D.P.R. 249/98 art. 4 punto 9-bis così come modificato dal DPR 235/2007).

I provvedimenti specifici per tipologia di infrazione sono riportati nel Regolamento di disciplina, allegato alla presente ePolicy.

Si richiama l'attenzione sulle possibili conseguenze penali e civili di eventuali riprese audio, video o fotografie, all'interno degli ambienti e dei contesti scolastici e successivamente diffuse con l'intento di ridicolizzare compagni, insegnanti e personale ATA o di commettere azioni riconducibili al reato del bullismo e/o del cyberbullismo.

Le responsabilità per atti di bullismo e cyberbullismo compiute da un minore di 14 anni possono ricadere anche su:

- i genitori, perché devono educare adeguatamente e vigilare, in maniera adeguata all'età del figlio, cercando di correggerne comportamenti devianti. Questa responsabilità generale persiste anche per gli atti compiuti nei tempi di affidamento alla scuola.

- "per quanto attiene alla responsabilità deontologica e professionale dei dirigenti, dei docenti e del personale ATA, si ricorda che il dovere di vigilanza sui comportamenti degli alunni sussiste in tutti gli spazi scolastici ed esige la tempestiva segnalazione alle autorità competenti di eventuali infrazioni, ed in particolare quando trattasi degli episodi di violenza sopra richiamati, dovere la cui inosservanza è materia di valutazione disciplinare" (DM 15 marzo 2007).

Le infrazioni alla ePolicy da parte del personale scolastico possono riguardare sia la mancata osservanza delle regole sulla gestione della strumentazione, sia la mancata sorveglianza e il mancato pronto intervento nel caso di infrazione da parte degli alunni. La gestione delle infrazioni in quest'ambito ricade nella disciplina contrattuale.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

La nostra ePolicy è coerente con quanto previsto dallo Statuto delle studentesse e degli studenti, dal Regolamento di Istituto e dal Patto di corresponsabilità educativa.

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 Dirigente Scolastico, con la collaborazione dell'Animatore digitale, del Team e dei Referenti del bullismo e cyber bullismo verificherà annualmente l'attuazione delle azioni previste nel Piano di azioni.

L'aggiornamento della Policy sarà curato dal Dirigente scolastico, dall'Animatore digitale, dal Team, dai Referenti del bullismo e cyberbullismo e dagli Organi Collegiali.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

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

Azioni da svolgere nei prossimi 3 anni:

- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti (nella scuola secondaria di primo grado)

- Organizzare 1 evento di presentazione e conoscenza dell’ePolicy rivolto ai genitori

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

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

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

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

L'Istituto Comprensivo S.P. Damiano si è dotato in questi ultimi anni di un curricolo per le competenze digitali, trasversale alle varie discipline.

Possedere una competenza digitale significa padroneggiare le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con "autonomia e responsabilità", con spirito critico, nel rispetto degli altri e sapendone prevenire ed evitare i pericoli. In questo senso, tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione.

Ogni anno, inoltre, l'Istituto aderisce a progetti del PAFT o realizza percorsi interni volti a sensibilizzare gli studenti e le studentesse ad una comunicazione corretta, anche tramite i dispositivi digitali, ad una gestione consapevole della propria reputazione digitale, ad una fruizione matura delle informazioni che circolano online e

al rispetto della privacy e dell'immagine altrui.

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.

I docenti, al fine di migliorare il proprio utilizzo delle TIC nonché di integrarle nella propria didattica, possono provvedere tramite autoaggiornamento, formazione personale o collettiva anche all'interno dell'Istituto, condivisione delle conoscenze e corsi di aggiornamento online.

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.

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

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

Il nostro piano d'azioni

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

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

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

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

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

In merito alla protezione dei dati personali, si fa riferimento a quanto previsto dal Decreto Legislativo del 30 giugno 2003, n.196 (cosiddetto Codice della Privacy), integrato dal D. Lgs. 10 agosto 2018, n. 101, e dal GDPR (General Data Protection Regulation) n. 679 del 2016.

I genitori possono consultare sul sito della scuola l'informativa sulla privacy. In funzione di progetti del PTOF ai genitori può essere richiesta l'autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori e liberatorie per l'utilizzo delle immagini secondo quanto previsto dal Codice in materia di protezione dei dati personali (Allegati). Il DS designa un responsabile della protezione dei dati (RDP). All'atto dell'iscrizione viene fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori, come ad esempio l'utilizzo di fotografie, video o altri materiali audiovisivi contenenti l'immagine e/o il nome del proprio figlio/a all'interno di attività educative e didattiche per scopi documentativi, formativi e informativi, durante gli anni di frequenza della scuola. L'autorizzazione non consente l'uso dell'immagine in contesti che pregiudichino la propria dignità personale ed il decoro e comunque per uso e/o fini diversi da quelli sopra indicati. Inoltre, in caso di partecipazioni a concorsi o manifestazioni l'Istituto richiede apposita autorizzazione, chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato all'interno di modulistica o sul proprio sito web istituzionale. Allo stesso modo sono forniti ai genitori, o ai tutori legali degli studenti, modelli di liberatoria per ogni attività interna ed esterna alla scuola (uscite, gite, interventi di esperti esterni…) e, negli ultimi anni, per la creazione e l'utilizzo di account istituzionale sulla piattaforma Google Workspace. Tale modulistica sarà allegata al presente documento di ePolicy.

Sia i docenti che gli alunni sono tenuti a custodire correttamente le proprie credenziali di accesso agli account istituzionali e ad effettuare correttamente il logout quando lasciano la propria postazione di lavoro.

https://www.icdamiano.edu.it/public/articoli/allegati/1/informativaprivacyperfoto.pdf

https://www.icdamiano.edu.it/public/articoli/allegati/1/liberatoriaprivacy.pdf

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.

L’accesso a Internet è possibile e consentito per la didattica in tutti i plessi della scuola dell’infanzia, della primaria e della secondaria di primo grado attraverso reti WiFi o cablaggio.

La Dirigenza e l’Amministrazione hanno una rete separata.

Tutte le Reti sono protette da password.

Gli alunni sono abilitati ad accedere a Internet sotto la supervisione dei docenti, principalmente utilizzando dispositivi della scuola già allacciati alla rete, preferibilmente accedendo al proprio account Google Workspace. Qualora l'accesso ad Internet dovesse avvenire attraverso dispositivi personali (es smartphone) esso dovrà avere luogo non attraverso la rete della scuola (di cui gli alunni non conoscono la password) ma utilizzando il traffico dati del dispositivo in uso. All'interno del dominio scolastico di Google WorkSpace gli alunni hanno delle limitazioni di navigazione e di accesso alle applicazioni, nonché la possibilità di comunicare via mail solamente all'interno del dominio stesso. L'account Google di ogni alunno/a ha la struttura nomecognome@damiano.istruzioneer.it e rimane attivo dal momento in cui la famiglia firma il consenso alla sua creazione fino al termine del percorso scolastico dell'alunno/a stesso/a all'interno del nostro IC. Successivamente, entro 60 giorni, l'account viene eliminato dall'amministratore della piattaforma e non è più recuperabile pertanto ogni alunno/a deve provvedere tempestivamente al trasferimento dei propri documenti ad altro account personale non appena termina il suo rapporto con la nostra scuola.

Per quel che concerne il comportamento da tenere nell'uso della piattaforma l'Istituto ha elaborato una netiquette valida per tutti gli utenti e riportata nei paragrafi precedenti.

Anche tutti i docenti e il personale ATA hanno un proprio account Google WorkSpace con la struttura n.cognome@damiano.istruzioneer.it; esso rimane attivo fino al termine del rapporto professionale con l'IC dopo di che viene sospeso/eliminato entro 60 giorni. Per questo motivo si consiglia di provvedere tempestivamente al trasferimento dei propri documenti ad altro account personale.

Per ottimizzare l'uso di Google WorkSpace for education si consiglia l'impiego del browser Google Chrome e, da cellulare e tablet, delle singole app (GMail, Drive, Classroom, Meet, ecc...) tenendo ben presente che queste ultime non dispongono di tutte le funzionalità offerte dalla piattaforma quando viene fruita tramite browser su un computer.

Ogni postazione di lavoro è munita di antivirus.

I docenti possono accedere alla propria sezione del registro elettronico con credenziali personali che devono essere custodite correttamente.

Sia gli alunni che il personale scolastico sono tenuti ad effettuare correttamente il logout dal proprio account personale prima di lasciare la propria postazione di lavoro e non devono salvare le credenziali di accesso ai propri account sui dispositivi della scuola.

3.3 - Strumenti di comunicazione online

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

La scuola ha un sito web raggiungibile all'indirizzo https://www.icdamiano.edu.it/ attraverso il quale comunica con docenti, famiglie e portatori di interesse esterni.

La scuola comunica con le famiglie anche attraverso il registro elettronico Argo in cui condivide informazioni sia didattiche che organizzative.

Docenti e alunni sono in contatto virtuale tramite la piattaforma Google WorkSpace for education dove avviene lo scambio di materiale, compiti e comunicazioni e all'interno della quale hanno anche luogo le videolezioni. In questi ultimi anni questa piattaforma ha permesso di affrontare le difficili condizioni didattiche conseguenti al dilagare dell'emergenza sanitaria ed ha anche permesso di mantenere la consuetudine dei colloqui con i genitori, seppur a distanza.

Nella comunicazione scuola-docenti tutte le comunicazioni, gli avvisi, le convocazioni, le circolari interne ecc. sono inviate/i tramite e-mail alla casella di posta istituzionale e/o sono pubblicate/i sulla bacheca del registro elettronico.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

La presente ***ePolicy*** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

Come da Regolamento d'Istituto agli studenti è fatto assoluto divieto di usare all'interno dell'Istituto scolastico, se non per scopi esclusivamente didattici autorizzati dal docente, smartphone e/o ogni altro apparato multimediale (mp3, ipod, ipad, notebook, fotocamera, videocamera, ecc…). Il divieto non si applica soltanto all'orario delle lezioni, ma all'intera permanenza dell'alunno all'interno della struttura scolastica (intervallo, cambio d'ora, ingresso ed uscita) e anche in occasione delle uscite didattiche o dei viaggi di istruzione, durante i quali l'utilizzo può essere autorizzato solo dal docente. I predetti dispositivi devono essere tenuti spenti e opportunamente custoditi all'interno dello zaino.

I docenti non possono utilizzare i telefoni cellulari durante l'orario di lezione se non per comprovata necessità lavorativa (per esempio la compilazione del registro per la mancata funzionalità dei dispositivi in dotazione nelle classi), a scopo didattico ed integrativo dei dispositivi scolastici disponibili o per motivi di emergenza. Durante il restante orario di servizio è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente mentre è permesso l'uso di altri dispositivi elettronici personali per attività funzionali all'insegnamento, ad integrazione di quelli scolastici disponibili.

Personale ATA: Durante l'orario di servizio al restante personale scolastico è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente.

Il nostro piano d'azioni

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

- 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

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

- 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.*

Così come stabilito all'interno del PTOF, l'Istituto si pone le seguenti finalità:

- contribuire allo sviluppo armonico e integrale della persona promuovendo la conoscenza, il rispetto e la valorizzazione delle diversità individuali, con il coinvolgimento attivo degli studenti e delle famiglie;

- formare ogni persona contribuendo all'elevazione culturale, sociale ed economica del Paese per rappresentare un fattore decisivo di sviluppo e di innovazione e per rimuovere gli ostacoli di ordine economico e sociale;
- contribuire alla crescita di persone consapevoli, critiche e capaci di scegliere; promuovere il concetto di cittadinanza europea attraverso lo sviluppo di una cultura della partecipazione, dell'incontro, del confronto e dell'inclusione.

Il progetto formativo portato avanti dall'Istituto si basa su:

- l'importanza della memoria storica e dell'educazione al rispetto della diversità in quanto facente parte di una società multietnica, fondata sulla convivenza e rispettosa delle reciproche differenze;
- lo sviluppo della creatività e di molteplici forme espressive, utilizzando non solo il linguaggio verbale, ma anche quelli non verbali;
- lo sviluppo di un atteggiamento critico nei confronti della realtà.

Per questo la nostra scuola non può esimersi dal mettere in atto misure volte alla prevenzione di atti di discriminazione, violenza e sopruso e alla crescita di cittadini consapevoli e responsabili.

La **prevenzione universale** viene perseguita attivando ogni anno progetti ad ampio raggio volti allo sviluppo delle competenze emotive e all'educazione ad un uso corretto delle nuove tecnologie, ricorrendo all'intervento di personale specializzato.

La scuola ha elaborato inoltre un progetto di Istituto di Educazione civica che ha tra i suoi obiettivi:

- riconoscere la propria identità, sapersi inserire in modo attivo e consapevole nella vita sociale e far valere al suo interno i propri diritti e bisogni riconoscendo al contempo quelli altrui, le opportunità comuni, i limiti, le regole, le responsabilità
- prevenire il disagio e promuovere la persona, favorire un clima di accoglienza e inclusione
- fornire una prima alfabetizzazione informatica e le prime competenze sull'uso dei sussidi multimediali; promuovere idonee prassi di utilizzo degli strumenti tecnologici con particolare riguardo alla prevenzione del cyberbullismo.

Ogni anno, in tutte le classi dell'IC, la programmazione dei docenti deve contenere iniziative e insegnamenti inerenti alle tematiche proposte all'interno di tale progetto con lo scopo di delineare un percorso di crescita verticale che porti gli alunni a gestire in modo responsabile e consapevole le proprie relazioni con gli altri e ad utilizzare in modo positivo e costruttivo le tecnologie informatiche.

I docenti, come già detto, hanno anche elaborato un curricolo verticale delle competenze digitali che chiama ogni docente a contribuire alla crescita di studenti capaci di muoversi negli ambienti virtuali in modo sicuro, corretto e rispettoso.

La scuola ha definito regole di disciplina per una adeguata convivenza civile che vengono lette in classe e commentate nei giorni di accoglienza delle prime classi di ogni ordine. Tali regole sono inoltre condivise con le famiglie al momento dell'iscrizione dei figli.

In ogni classe della scuola secondaria è affisso il Manifesto della comunicazione non ostile che può accompagnare riflessioni di classe in ogni momento.

Sia gli alunni che i genitori hanno accesso, all'occorrenza, al servizio di Supporto psicologico dato da personale specializzato all'interno della scuola.

Quando possibile la scuola organizza momenti di formazione/informazione anche per le famiglie ricorrendo all'intervento di esperti esterni.

Gli interventi di prevenzione universale riguardano tutti gli studenti e tutte le famiglie, partendo dal presupposto che tutti i ragazzi siano potenzialmente a rischio.

Azioni di **prevenzione selettiva** e/o di **prevenzione indicata** vengono invece attuate quando è stato individuato un rischio specifico o un caso particolare che richiedono di intervenire per ridurre il rischio di comportamenti problematici. Generalmente intervengono in primis i docenti che possono poi chiedere il supporto dello psicologo della scuola, dei referenti per il bullismo e il cyberbullismo, di colleghi competenti e del dirigente; anche la famiglia risulta un importante interlocutore/ collaboratore per la gestione di tali situazioni.

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).

La Legge 71/2017 introduce anche un provvedimento di carattere amministrativo per gli autori di atti di cyberbullismo, la procedura di AMMONIMENTO da parte del Questore: il minore autore può essere convocato dal Questore e ammonito se ritenuto responsabile delle azioni telematiche.

Chi compie atti di bullismo e cyberbullismo può anche essere, comunque, responsabile di reati penali e danni civili.

Secondo il codice penale italiano i comportamenti penalmente rilevanti in questi casi sono:

- percosse (art. 581),
- lesione personale (art. 582),
- ingiuria (art. 594),
- diffamazione (art. 595),
- violenza privata (art. 610),
- minaccia (art. 612),
- danneggiamento (art. 635).

Per poter avviare un procedimento penale nei confronti di un minore è necessario:

- che abbia almeno compiuto 14 anni;
- che, comunque, anche se maggiore di 14 anni, fosse cosciente e volente al

momento del comportamento, cioè in grado di intendere e volere (tale non sarebbe, per esempio, un ragazzo con degli handicap psichici).

Le responsabilità per atti di bullismo e cyberbullismo compiute dal minorenne possono ricadere anche su:

- i genitori, perché devono educare adeguatamente e vigilare, in maniera adeguata all'età del figlio, cercando di correggerne comportamenti devianti. Questa responsabilità generale persiste anche per gli atti compiuti nei tempi di affidamento alla scuola (culpa in educando);
- gli insegnanti e la scuola: perché nei periodi in cui il minore viene affidato all'Istituzione scolastica il docente è responsabile della vigilanza sulle sue azioni e ha il dovere di impedire comportamenti dannosi verso gli altri/e ragazzi/e, insegnanti e personale scolastico o verso le strutture della scuola stessa. A pagare in primis sarà la scuola, che poi potrà rivalersi sul singolo insegnante. La responsabilità si estende anche a viaggi, gite scolastiche, manifestazioni sportive organizzate dalla scuola (culpa in vigilando);
- esiste poi una culpa in organizzando, che si ha quando la scuola non mette in atto le azioni previste per la prevenzione del fenomeno o per affrontarlo al meglio (così come previsto anche dalla normativa vigente).

La nostra scuola attua quotidianamente una attenta osservazione volta all'individuazione e/o alla prevenzione di situazioni di disagio e di comportamenti non corretti e/o prevaricanti (avvalendosi anche del supporto di psicologi), attiva ogni anno progetti e/o interventi formativi rivolti ad alunni e genitori con l'intenzione di contribuire a stimolare il rispetto reciproco, l'empatia e l'accettazione delle diversità e ad aumentare la consapevolezza nell'uso delle nuove tecnologie. In un'ottica di prevenzione l'Istituto ha elaborato la propria Netiquette, ossia una raccolta di regole di buon comportamento online, ha integrato il proprio Regolamento di Istituto con scenari riguardanti casi di uso non corretto dei dispositivi elettronici e i docenti della scuola dell'Infanzia, della scuola Primaria e di quella Secondaria di primo grado hanno elaborato il curricolo verticale delle competenze digitali per accompagnare i bambini e i ragazzi lungo un efficace percorso di formazione in questo ambito.

Dall'a.s. 2017/2018 è stato nominato il Referente per il bullismo e il cyberbullismo che, dopo aver seguito percorsi di formazione, ha promosso all'interno della scuola progetti rivolti principalmente agli alunni della scuola secondaria e volti all'educazione ad un uso consapevole e responsabile delle nuove tecnologie.

Dall'a.s. 2021/2022, in aggiunta a quello già presente, sono stati nominati altri due referenti così ora la scuola ha un referente per ogni plesso della scuola primaria (2) e secondaria di primo grado (1).

I referenti hanno elaborato il Protocollo per la gestione dei casi di bullismo e cyberbullismo che si pone come documento di riferimento sia per la conoscenza della tematica nei suoi diversi aspetti, sia per la gestione vera e propria dei casi. Secondo tale protocollo non solo il personale scolastico ma anche gli alunni e i genitori possono segnalare eventuali situazioni di presunto bullismo e cyberbullismo e, nella fase di attuazione degli interventi, possono essere coinvolte anche le famiglie oltre al personale scolastico e agli esperti esterni.

Il Protocollo è stato presentato ai docenti dopo che gli stessi sono stati invitati a partecipare ad un percorso di formazione interna tenuto dallo psicologo della scuola.

Nell'a.s. 2021/2022 è stato strutturato un progetto verticale sul potenziamento delle competenze emotive e sull'approfondimento delle tematiche inerenti il bullismo e il cyberbullismo che prevede l'intervento dello psicologo della scuola nelle classi IV e V della primaria e I, II e III della secondaria. Le famiglie sono state invitate a partecipare ad un incontro serale online sui rischi legati alla Rete e al mondo virtuale in cui il relatore era lo psicologo della scuola.

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.

La scuola, all'interno del proprio PTOF, prevede progetti volti alla crescita di cittadini consapevoli, tolleranti, inclusivi, empatici. L'attenzione verso questi aspetti è sempre alta e, al di là delle attività strutturate, ogni occasione è valida per fare riflessioni, da parte di tutti i docenti. Come già detto in ogni classe della scuola secondaria è affisso il Manifesto della comunicazione non ostile, a disposizione di ogni docente per eventuali approfondimenti con la classe.

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?

L'Istituto, nell'ambito degli interventi sul benessere digitale di cui si è già parlato affronta anche le problematiche relative alla dipendenza da Internet e gioco online; questo è un argomento trasversale, viene trattato quando si parla di cittadinanza digitale, di cyberbullismo, di uso integrativo e non sostitutivo dei dispositivi e della Rete.

Data la grande attualità del tema e la sua e rilevanza, soprattutto tra i ragazzi e le ragazze nella fascia di età della scuola primaria/ secondaria di primo grado, l'Istutito si pone comunque l'obiettivo di inserire nella proposta formativa dei prossimi anni interventi specifici sull'argomento che portino, tra le altre cose, a riflettere insieme su: come trascorri il tempo on line? Quando aggiunge valore alla tua vita e quando ti fa perdere tempo? Quale atteggiamento potrei cambiare quando sono online? Che ruolo ha e deve avere la tecnologia (internet o il gioco) nella vita?

Se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi.

4.5 - Sexting

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

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

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.

Il Protocollo per la gestione delle situazioni di bullismo e cyberbullismo del nostri Istituto dedica spazio anche a questo problema prevedendo che “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 rivolgersi al più vicino Compartimento di Polizia Postale e delle Comunicazioni con l’obiettivo di ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

Se si ravvisa un rischio per il benessere psicofisico delle persone minorenni coinvolte sarà opportuno rivolgersi ad un servizio deputato ad offrire un supporto psicologico anche passando per una consultazione presso il medico di base o il 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.). E’ da evitare la ricerca pro attiva online delle immagini da parte degli stessi ragazzi/e, pena il rischio di passibilità di reato per detenzione di materiale pedopornografico.

Sarà infine necessario che uno o più componenti del Team dell’emergenza si occupino di proporre in classe attività e approfondimenti su cosa prevede la legge sulla diffusione di materiale pedopornografico, sull’educazione all’affettività, sui rischi legati ad un uso non consapevole della Rete e sul rispetto della privacy”.

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.

La problematica dell'adescamento online (come quella del sexting) si inquadra in uno scenario più ampio di scarsa educazione emotiva, sessuale e di assenza di competenza digitale.

Al fine di prevenire casi di adescamento online è opportuno, pertanto, accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli emotivamente più sicuri e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. Fondamentale quindi, come sappiamo, è portare avanti un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è).

Alcuni consigli per i nostri alunni e i nostri figli:

1. Non fidarti di chi vuole sapere troppe cose.

2. Non dare nessuna informazione su di te, sulla tua famiglia o sui tuoi amici ed evita di inviare foto personali a persone che non conosci. In Rete è facile perdere il controllo delle informazioni e non si può mai sapere chi entrerà in loro possesso e per quanto tempo circoleranno!

3. Ricordati sempre che è facile mentire quando si è on-line: alcune persone possono fingersi tuoi coetanei, quando in realtà non lo sono, o mascherare le reali intenzioni

per cui sono entrate in contatto con te.

4. Incontrare qualcuno che si è conosciuto solo tramite la Rete non è una buona idea, anche se questa persona ti ha inviato foto o se tu l'hai vista tramite una webcam: le immagini potrebbero essere contraffatte!

5. Se qualcuno ti mette a disagio o ti propone azioni che ritieni inadeguate o che i tuoi genitori ti hanno detto di non compiere, bloccalo immediatamente interrompendo i contatti.

6. Condividi: se ricevi o vedi qualcosa che ti mette a disagio, parlane con i tuoi genitori o con i tuoi insegnanti.

Il Protocollo per la gestione delle situazioni di bullismo e cyberbullismo del nostro Istituto dedica spazio anche a questo problema prevedendo che: "Qualora un adulto dovesse sospettare o avere certezza rispetto alla possibilità che un minore sia coinvolto o si stia coinvolgendo in una situazione di questo tipo, è importante che non si sostituisca al minore stesso, ad esempio nel rispondere all'adescatore. È fondamentale che venga tenuta traccia degli scambi intercorsi (es. salvare le conversazioni, fare degli screenshots) rivolgendosi il prima possibile alla Polizia Postale e delle Comunicazioni. In seguito alla tempestiva gestione degli aspetti strettamente inerenti la Rete e la denuncia, è importante anche valutare la possibilità di rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire al minore un adeguato supporto di tipo psicologico o psichiatrico. Sarà infine necessario che uno o più componenti del Team dell'emergenza si occupino di proporre in classe attività sulla fiducia e sull'affettività e approfondimenti su quanto previsto dalla normativa e sulle differenze tra relazioni reali e relazioni virtuali."

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.

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.

Studi in materia dimostrano come l'utilizzo di materiale pedopornografico possa essere propedeutico all'abuso sessuale agito ed è quindi fondamentale, in termini preventivi, intervenire per ridurre l'incidenza di tale possibilità.

Se si ravvisa un rischio per il benessere psicofisico dei/lle bambini/e, ragazzi/e coinvolte nella visione di questi contenuti sarà opportuno inoltre ricorrere a 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.

Prevenire significa innanzitutto favorire e potenziare tutte quelle condizioni individuali, familiari e sociali che proteggono un bambino, ostacolando il verificarsi di un abuso. È importante ricordare che una prevenzione efficace parte, ancor prima che da interventi strutturati e focalizzati sul tema dell'abuso o della pedofilia, da un contesto educativo e familiare capace di dare ascolto al bambino e ai suoi bisogni, nelle differenti fasi evolutive.

Poiché il primo dovere di un genitore è quello di proteggere i propri figli, ricordiamo di seguito alcuni SUGGERIMENTI UTILI PER LE FAMIGLIE:

1. costruite con vostro figlio le premesse per un dialogo sincero, mostrandogli sempre la vostra disponibilità ad ascoltarlo e ad accogliere le sue emozioni;

2. interessatevi e partecipate alle attività che svolge, impegnatevi a conoscere le persone e i luoghi che frequenta. È importante prestargli/le attenzione mentre gioca, mentre fa i compiti, mentre guarda la tv; cercate momenti per stare insieme, anche se il tempo a disposizione può essere poco, lasciando per un po' da parte altri pensieri e problemi;

3. prestate attenzione anche ai piccoli cambiamenti che avvengono nel suo comportamento e nei suoi atteggiamenti, ancor più se improvvisi; solo così potrete accorgervi se qualcosa lo/a turba;

4. evitate che resti solo/a e privo/a di supervisione;

5. scegliete con attenzione a chi affidarlo/la (ad esempio, babysitter, vicini di casa, etc.);

6. mantenete un dialogo sempre aperto con gli insegnanti e la scuola;

7. stabilite con lui/lei alcune semplici regole di sicurezza da seguire sempre (ad esempio, non accettare inviti da parte di sconosciuti, informare regolarmente i genitori se c'è qualcuno che gli/ le offre dei regali o gli/le chiede di mantenere dei segreti, etc.).

Per quanto riguarda la prevenzione e la gestione di tali situazioni a scuola, qualsiasi intervento deve essere focalizzato su:

• Riconoscimento di possibili situazioni di rischio, distinguendole da situazioni innocue

• Favorire il dialogo col minore garantendogli la riserbatezza in merito a particolari confidenze

• Riferire l'eventuale abuso a Dirigente Scolastico e Forze dell'ordine

• Rassicurare il bambino e l'adolescente nel caso in cui si senta responsabile o in colpa per quanto accaduto.

L'argomento pedopornografia è molto delicato: se da una parte gli adulti, i genitori e i docenti sono tenuti a documentarsi e a conoscere il fenomeno, interventi diretti ai ragazzi non sono sempre opportuni. La nostra scuola ritiene che i più giovani debbano acquisire competenze in grado di orientarli e guidarli nelle loro scelte anche online grazie ai percorsi di educazione civica e in particolare di educazione all'affettività.

Il nostro piano d'azioni

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

□ 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/lle studenti/studentesse, con il coinvolgimento di esperti.

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

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

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

□ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per

segnalare la presenza di materiale pedopornografico online.

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.

All'interno del Protocollo per la gestione delle situazioni di bullismo e cyberbullismo (Allegato al presente capitolo) sono definite le modalità di segnalazione di casi di presunto disagio. La segnalazione può essere fatta dagli studenti, dalle famiglie e dal personale scolastico in vari modi:

- compilando il modulo cartaceo disponibile e scuola e inserendolo nell'apposita scatola che viene periodicamente controllata dal referente per il bullismo e il cyberbullismo
- inviando via e-mail all'indirizzo bullismo@damiano.istruzioneer.it il modulo che si può scaricare dal sito della scuola e allegato alla presente ePolicy
- comunicando la situazione ad un adulto di riferimento interno alla scuola.

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.

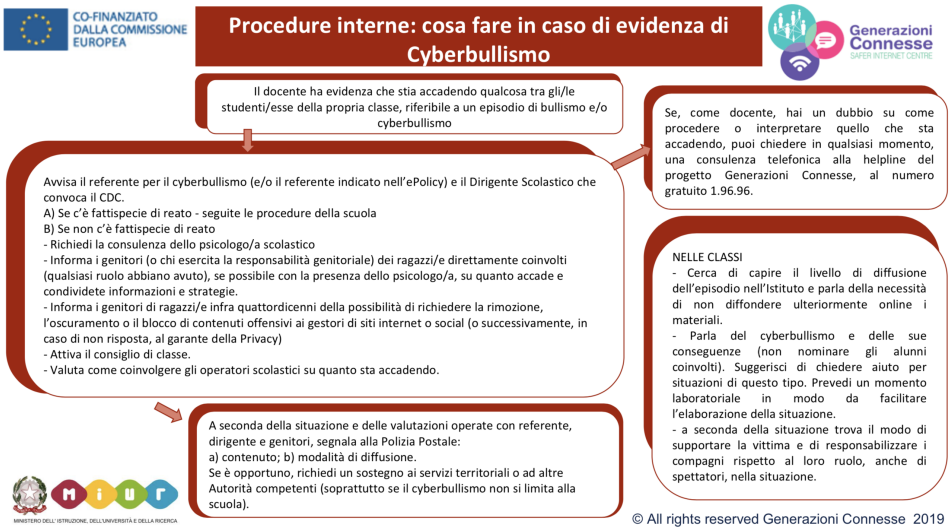
- **Polizia Postale e delle Comunicazioni**: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche 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.

All'interno del Protocollo per la gestione delle situazioni di bullismo e cyberbullismo (Allegato al presente capitolo) è inserita una scheda che riporta il contatto dei principali attori sul territorio a cui rivolgersi in caso di necessità:

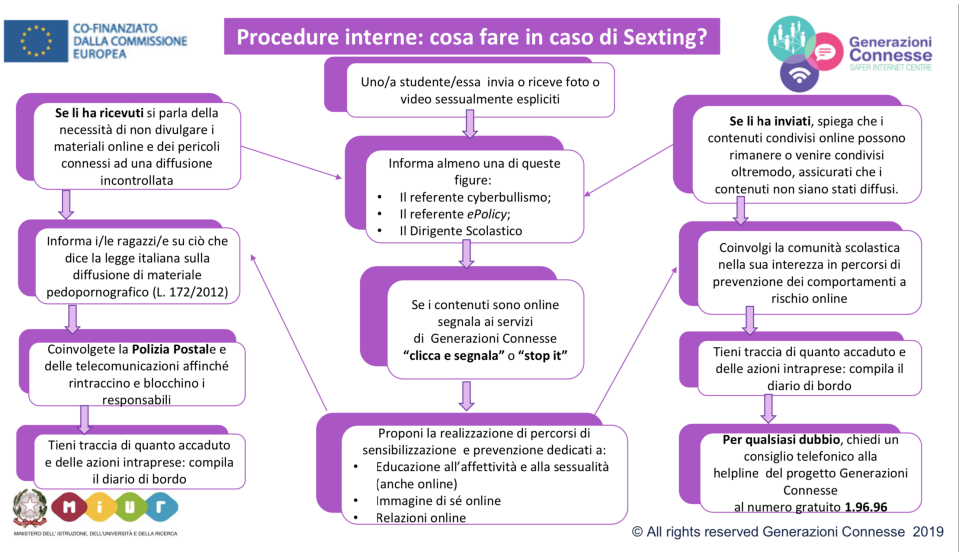
ENTE/ SERVIZIO	**CONTATTO**
SERVIZI SOCIALI	0544 482550
PRONTO SOCORSO	118
POLIZIA POSTALE	0544 284678
CARABINIERI	112
HELP LINE DI GENERAZIONI CONNESSE (Telefono Azzurro)	19696

5.4. - Allegati con le procedure

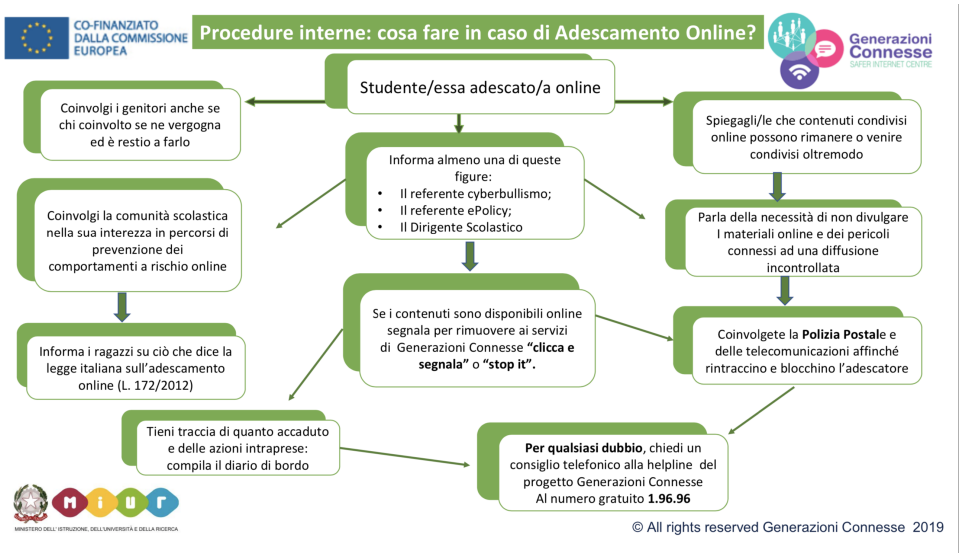
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



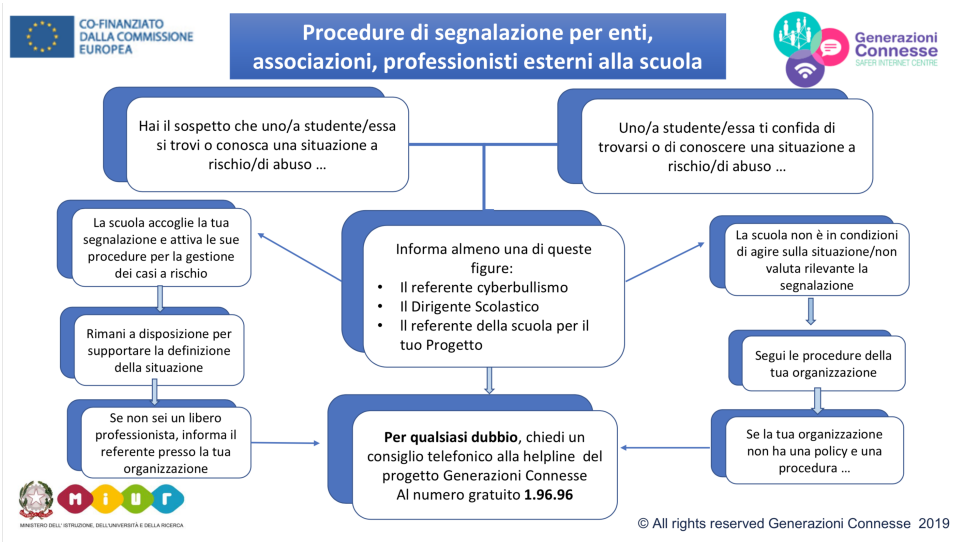
Procedure interne: cosa fare in caso di sexting?



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

https://www.icdamiano.edu.it/public/articoli/allegati/1/protocolloemergenzebullismo_cyberbullism.pdf

https://www.icdamiano.edu.it/public/articoli/allegati/1/primasegnalazionedeicasidipresuntobullis.pdf

https://www.icdamiano.edu.it/public/articoli/allegati/1/23giugnoregolamentonuovomedie3.pdf

Il nostro piano d'azioni

Al termine dell'anno scolastico si verificherà l'efficacia del Protocollo e il livello di fruibilità da parte delle parti interessate:

- ai docenti, alle famiglie e agli alunni verrà sottoposto un semplice questionario in formato Google Moduli
- verranno conteggiati i casi segnalati e verrà verificata quale percentuale di essi è stato seguito per l'intero iter previsto

- verranno verificati i risultati del monitoraggio dei casi.