

DIREZIONE DIDATTICA STATALE III CIRCOLO - "ALDO MORO"-AFRAGOLA
Prot. 0007859 del 24/10/2023
IV (Uscita)



Documento di ePolicy

NAEE105003

TERZO CIRCOLO DIDATTICO

ALDO MORO

VIA UGO LA MALFA - 80021 - AFRAGOLA - NAPOLI (NA)

FRANCESCALAURA CASILLO

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

1. Presentazione dell'ePolicy

1. Scopo dell'ePolicy
2. Ruoli e responsabilità
3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
5. Gestione delle infrazioni alla ePolicy
6. Integrazione dell'ePolicy con regolamenti esistenti
7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

2. Formazione e curriculum

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

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

1. Protezione dei dati personali
2. Accesso ad Internet
3. Strumenti di comunicazione online
4. Strumentazione personale

4. Rischi on line: conoscere, prevenire e rilevare

1. Sensibilizzazione e prevenzione
2. Cyberbullismo: che cos'è e come prevenirlo
3. Hate speech: che cos'è e come prevenirlo
4. Dipendenza da Internet e gioco online
5. Sexting
6. Adescamento online
7. Pedopornografia

5. Segnalazione e gestione dei casi

1. Cosa segnalare
2. Come segnalare: quali strumenti e a chi
3. Gli attori sul territorio per intervenire
4. Allegati con le procedure

Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

FINALITÀ

Obiettivo dell'e-policy è quello di orientare la nostra scuola nell'individuazione e prevenzione dei comportamenti devianti, troppo spesso ignorati o minimizzati.

Il bullismo e il cyberbullismo devono essere conosciuti e combattuti da tutti in tutte le forme, così come previsto:

- dagli art. 3-33-34 della Costituzione Italiana;
- dalla Direttiva MIUR n.16 del 5 febbraio 2007 recante “Linee di indirizzo generali e azioni a livello nazionale per la prevenzione e la lotta al bullismo”;
- dalla direttiva MPI n. 30 del 15 marzo 2007 recante “*Linee di indirizzo ed indicazioni in materia di utilizzo di ‘telefoni cellulari’ e di altri dispositivi elettronici durante l’attività didattica, irrogazione di sanzioni disciplinari, dovere di vigilanza e di corresponsabilità dei genitori e dei docenti*”;
- dalla direttiva MPI n. 104 del 30 novembre 2007 recante “Linee di indirizzo e chiarimenti interpretativi ed applicativi in ordine alla normativa vigente posta a tutela della privacy con particolare riferimento all’utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire e/o divulgare immagini, filmati o registrazioni vocali”;
- dalla direttiva MIUR n.1455/06;
- dalle LINEE DI ORIENTAMENTO MIUR, Aprile 2015, per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo.
- dal D.P.R. 249/98 e 235/2007 recante “Statuto delle studentesse e degli studenti”;
- dagli artt. 581-582-594-595-610-612-635 del Codice Penale;

- dagli artt. 2043-2047-2048 Codice Civile;
 - dalla legge 29 maggio 2017, n. 71;
 - dalle Nuove LINEE DI ORIENTAMENTO MIUR, Ottobre 2017, per azioni di prevenzione e di contrasto al bullismo e al cyber bullismo;
 - dal Regolamento di Istituto del Terzo Circolo Aldo Moro Afragola (Na).
-

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.

RESPONSABILITÀ DELLE VARIE FIGURE SCOLASTICHE E DEI FAMILIARI

1. IL DIRIGENTE SCOLASTICO:

- adotta e sostiene una politica scolastica che faciliti il riconoscimento del bullismo e del cyberbullismo e la loro riduzione attivando progetti di prevenzione e contrasto dei fenomeni;
- prevede azioni culturali ed educative rivolte agli studenti, per acquisire le competenze necessarie all'esercizio di una convivenza civile e consapevole;
- favorisce la discussione all'interno della scuola, attraverso i vari organi collegiali, creando i presupposti di regole condivise di comportamento per il contrasto e prevenzione dei fenomeni del bullismo e cyberbullismo;
- individua, attraverso il Collegio dei Docenti, i docenti in qualità di Referenti d'Istituto per la prevenzione e il contrasto al bullismo e cyberbullismo;
- qualora venga a conoscenza di atti di bullismo/cyberbullismo (salvo che il fatto costituisca reato) informa tempestivamente i soggetti che esercitano la responsabilità genitoriale o i tutori dei minori coinvolti e attiva adeguate azioni di carattere educativo.

2. I REFERENTI D'ISTITUTO PER LA PREVENZIONE E IL CONTRASTO AL BULLISMO E CYBERBULLISMO:

- coordinano e promuovono iniziative di informazione, di sensibilizzazione e di prevenzione del bullismo e del cyberbullismo rivolte alle famiglie, agli studenti e al personale scolastico, coinvolgendo primariamente i servizi socio-educativi presenti sul territorio attraverso progetti d'istituto, corsi di formazione, seminari, dibattiti, finalizzati all'educazione e all'uso consapevole della rete internet;
- promuovono attività progettuali connesse all'utilizzo delle tecnologie informatiche, aventi carattere di continuità tra i diversi gradi di istruzione o progetti elaborati da reti di scuole in collaborazione con enti locali, servizi territoriali, organi di polizia, associazioni ed enti;
- Curano rapporti di rete fra scuole per eventuali convegni/seminari/corsi e per la giornata mondiale sulla Sicurezza in Internet, il "Safer Internet Day";
- aggiornano, coadiuvati da una Commissione appositamente nominata, il Regolamento d'Istituto e il Patto di Corresponsabilità, integrando specifici riferimenti a condotte di cyberbullismo e a relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- coordinano le attività di prevenzione ed informazione sulle sanzioni previste dal Regolamento d'Istituto nei casi di bullismo e cyberbullismo, navigazione online a rischio, e sulle responsabilità di natura civile e penale, anche con eventuale affiancamento di genitori e studenti.

3. IL CONSIGLIO D'ISTITUTO:

- approva e adotta il Regolamento per la prevenzione e il contrasto al bullismo e cyberbullismo;
- qualora a scuola si verificano azioni di bullismo e/o casi di diffusione a terzi di foto/audio/video in violazione delle norme sulla privacy, si pronuncia - previa verifica della sussistenza di elementi concreti e precisi dai quali si evinca la responsabilità disciplinare dello studente - sulle sanzioni che prevedono lavori socialmente utili alla comunità scolastica.

4. IL COLLEGIO DEI DOCENTI:

- promuove scelte didattiche ed educative, anche in collaborazione con altre scuole in rete, per la prevenzione del fenomeno del bullismo e cyberbullismo;
- prevede all'interno del PTOF corsi di aggiornamento e formazione in materia di Cittadinanza digitale e di prevenzione dei fenomeni di bullismo e cyberbullismo;
- progetta azioni culturali ed educative rivolte agli studenti, per acquisire le competenze necessarie all'esercizio di una Cittadinanza digitale consapevole; o coinvolge, nella prevenzione e contrasto al fenomeno del bullismo e del cyberbullismo, tutte le componenti della comunità scolastica.

5. IL CONSIGLIO DI CLASSE/TEAM DOCENTI:

- favorisce un clima collaborativo in classe, promuovendo l'integrazione, la cooperazione e l'aiuto tra par

- pianifica attività didattiche e/o integrative finalizzate al coinvolgimento attivo e collaborativo degli studenti e all'approfondimento di tematiche che favoriscano la riflessione e la presa di coscienza di valori di convivenza civile quali: rispetto, uguaglianza e dignità, intercultura;

- nelle relazioni con le famiglie propone progetti di educazione alla legalità e alla cittadinanza attiva.

6. L' ANIMATORE DIGITALE:

- supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali;

- promuove percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale";

- individua soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;

- organizza laboratori formativi che stimolano la partecipazione di studenti, famiglie e altri attori del territorio (workshop, coding ecc.);

- coinvolge il più possibile tutta la comunità scolastica nella partecipazione ad attività e progetti attinenti il PNSD;

- monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola;

- ha il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione anche a distanza; DAD/DDI);

- collabora con il Dirigente scolastico nella gestione dei casi di violazione o illecito online.

6. IL DOCENTE:

- intraprende azioni congruenti con l'utenza del proprio ordine di scuola, tenuto conto che l'istruzione ha un ruolo fondamentale sia nell'acquisizione e rispetto delle norme relative alla convivenza civile, sia nella trasmissione dei valori legati ad un uso responsabile di internet.

-valorizza, nell'attività didattica, modalità di lavoro di tipo cooperativo e spazi di riflessioni adeguati al livello di età degli alunni;

-potenzia le abilità sociali nei bambini e/o nei ragazzi;

-organizza attività, incontri, riunioni con alunni e genitori per segnalare e parlare insieme di eventuali situazioni di prepotenza che si possono verificare in classe o a scuola, per cercare insieme possibili soluzioni;

- informa gli alunni sui rischi presenti in Rete, sollecitandone un utilizzo consapevole, in modo che Internet possa rimanere per i ragazzi una fonte di divertimento e apprendimento.

7. I GENITORI:

-partecipano attivamente alle azioni di formazione/informazione, istituite dalle scuole, sui comportamenti sintomatici del bullismo e del cyberbullismo;

-sono attenti ai comportamenti dei propri figli;

-vigilano sull'uso delle tecnologie da parte dei ragazzi, con particolare attenzione ai tempi, alle modalità, agli atteggiamenti conseguenti (i genitori dovrebbero allertarsi se uno studente, mostra stati depressivi, ansiosi o paura);

-conoscono le azioni messe in campo dalla scuola e collaborano secondo le modalità previste dal Patto Educativo di Corresponsabilità;

-conoscono il codice di comportamento dello studente;

- conoscono le sanzioni previste da Regolamento d'Istituto nei casi di bullismo, cyberbullismo.

7. DIRETTORE DEI SERVIZI GENERALI ED 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

8. GLI ALUNNI:

sono coinvolti nella progettazione e nella realizzazione delle iniziative scolastiche, al

fine di favorire un miglioramento del clima relazionale; in particolare, dopo opportuna formazione, possono operare come tutor per altri studenti;

- imparano le regole basilari per rispettare gli altri, quando sono connessi alla rete, facendo attenzione alle comunicazioni (e-mail, sms, mms) che inviano;

- non è loro consentito, durante le attività didattiche o comunque all'interno della scuola, acquisire – mediante telefonini cellulari o altri dispositivi elettronici - immagini, filmati o registrazioni vocali, se non per finalità didattiche e sempre previo consenso del docente. La divulgazione del materiale eventualmente acquisito all'interno dell'istituto è utilizzabile solo per fini esclusivamente personali di studio o documentazione, e, comunque, nel rispetto del diritto alla riservatezza di tutti;

-durante le lezioni o le attività didattiche il cellulare deve essere spento; non devono essere usati cellulari, giochi elettronici e riproduttori di musica, se non per finalità didattiche, previo consenso del docente;

-sono tenuti a rispettare il Regolamento d'Istituto e le relative sanzioni disciplinari.

9. PERSONALE ATA/TECNICO-AMMINISTRATIVO

Il personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste, ossia di tipo amministrativo contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il dirigente scolastico e con il personale docente tutto. Il personale ATA è coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo insieme ad altre figure e raccoglie, verifica e valuta le informazioni inerenti possibili casi di bullismo/cyberbullismo.

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).

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola:

-condividono la politica della stessa riguardo all'uso consapevole della Rete e delle TIC;

-erogano le attività educative solo a seguito di autorizzazione formale del Dirigente scolastico;

-promuovono comportamenti sicuri, la sicurezza online e assicurano la protezione dei dati personali e sensibili degli studenti e delle studentesse durante le attività che si svolgono insieme.

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.

La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet sarà discussa negli organi collegiali (Consiglio di Istituto, Collegio dei Docenti). Il documento viene redatto dal *Gruppo di lavoro per l'epolicy* secondo le linee recepite. Le regole relative alla sicurezza digitale e all'accesso a internet sono approvate dagli Organi preposti che possono apportare eventuali modifiche e integrazioni. Il documento una volta approvato è reso pubblico, inserito all'interno del PTOF e consultabile all'utenza sul sito dell'istituto: <https://www.aldomorocd.edu.it/>

L'E-Policy di Istituto si applica a tutte le figure che possono avere accesso alle reti interne della scuola e a coloro che, in qualità di genitori o tutori legali, sono coinvolti nella vigilanza domestica. Il documento viene condiviso con gli studenti e le studentesse, i genitori e tutto il personale della scuola. Esso si integra pienamente con gli obiettivi e i contenuti presenti nel:

-PTOF

-Regolamento interno di istituto che ha recepito le indicazioni della L. 71/2017

-Patto di corresponsabilità tra scuola, genitori ed alunni

GLI STUDENTI E LE STUDENTESSE sono informati/formati all'uso responsabile e sicuro della rete attraverso la lettura e la condivisione, da parte degli insegnanti di classe, del documento E-policy, del Regolamento di Istituto e per la sicurezza on line e del Patto di corresponsabilità.

I GENITORI degli alunni sono informati/formati sulla politica della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet tramite la condivisione del documento E-policy sul sito web della scuola. All'atto dell'iscrizione o all'inizio dell'anno scolastico la scuola chiede ai genitori degli studenti la sottoscrizione del Regolamento, il consenso informato all'uso di internet, la liberatoria per la pubblicazione di elaborati di vario genere e/o fotografie per il loro figlio. Allo scopo di favorire la collaborazione scuola-famiglia, verranno organizzati incontri di vario genere (assemblee, seminari, riunioni) con esperti interni o personale esterno durante i quali si farà riferimento al presente documento allo scopo di sensibilizzare sul tema, accogliere eventuali segnalazioni e suggerimenti utili alla implementazione e revisione annuale della policy.

IL PERSONALE DELLA SCUOLA viene informato/formato sulla politica della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet tramite materiale informativo e riunioni istituzionali (Consigli di classe, interclasse/intersezione, Collegio dei Docenti). Le norme adottate dall'Istituto scolastico in materia di sicurezza nell'utilizzo del digitale saranno rese note tramite pubblicazione del presente documento sul sito web della scuola. Il personale è reso consapevole del fatto che sono sanzionabili le condotte non in linea con il codice di comportamento dei dipendenti pubblici e con la policy di Istituto.

ORGANIZZAZIONI E SOGGETTI ESTERNI (figure professionali, collaboratori, associazioni) coinvolti in progetti, laboratori e attività devono prendere visione di tutti i documenti proposti dall'Istituto in materia di rispetto della privacy e sicurezza on line e sottoscriverli preliminarmente all'avvio dei programmi con gli studenti e le studentesse, in classe o da remoto.

Nello specifico è importante:

- **condividere e comunicare il documento agli studenti e alle studentesse** significa dare loro una base di partenza per un uso consapevole e maturo dei dispositivi e della tecnologia informatica; dare loro regole condivise di sicurezza circa il comportamento da tenere a scuola e nei contesti extrascolastici; dare loro elementi per poter riconoscere e quindi prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e.
- **è importante condividere e comunicare il documento al personale scolastico** in modo da poter orientare tutte le figure sui temi in oggetto, a partire da un uso corretto dei dispositivi e della Rete in linea anche con il codice di comportamento dei pubblici dipendenti;
- **è fondamentale condividere e comunicare il documento ai genitori** sul sito istituzionale della scuola, nonché tramite momenti di formazione specifici e durante gli incontri scuola-famiglia.

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.

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 rischi effettivi che si possono correre a scuola nell'utilizzo delle TIC da parte degli alunni derivano da un uso non corretto del telefono cellulare personale o dello smartphone, dei pc della scuola collegati alla rete. Il telefono cellulare o lo smartphone non sono chiesti dalla scuola, in quanto non indispensabili in ambito scolastico, ma vengono forniti dai genitori degli alunni per mantenere la comunicazione diretta con i figli anche fuori dal contesto scolastico. Evitando la sorveglianza degli insegnanti, attraverso i telefoni cellulari o gli smartphone, con particolari applicazioni e di collegamento ad internet, oltre che parlare e scrivere messaggi con i genitori, gli alunni potrebbero anche scaricare e spedire foto personali, intime, sia proprie che di altri; così come pure video con contenuti indecenti o violenti, o accedere a internet e a siti non adatti ai minori, ascoltare musica e giocare con i videogiochi non consigliati ai minori, leggere la posta elettronica e comunicare o chattare con sconosciuti, inviare o ricevere messaggi molesti e minacciosi. Sempre schivando la sorveglianza degli insegnanti, gli alunni potrebbero correre gli stessi rischi a scuola anche con l'utilizzo dei pc del

laboratorio informatico e con un accesso non controllato a Internet.

Sono previsti pertanto da parte dei docenti provvedimenti “disciplinari” proporzionati all’età e al comportamento quali:

- Il richiamo verbale
- Il richiamo scritto
- La convocazione dei genitori
- La segnalazione agli assistenti sociali
- La segnalazione alle autorità competenti in caso di reati.

Al contempo sono previsti interventi educativo/formativo di prevenzione e gestione dei conflitti e di quanto afferente alla sfera affettiva/emozionale.

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 per obiettivi e contenuti con Il PTOF ed regolamento di Istituto. Il 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.

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 è responsabile dell'implementazione della ePolicy all'interno dell'Istituto. Questo documento verrà aggiornato periodicamente e secondo necessità dovuta a cambiamenti significativi. Le modifiche saranno concordate con il referente, l'animatore digitale, la commissione e approvate dal Collegio dei Docenti e dal Consiglio di Circolo.

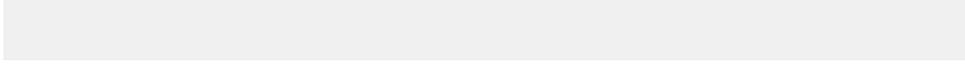
Il nostro piano d'azioni

Azioni da sviluppare 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 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare una presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare una presentazione del progetto Generazioni Connesse rivolto ai genitori.
- 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 sviluppare 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(condivisione con il team digitale e con il gruppo di lavoro per la stesura dell'epolicy.
- 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. 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 curriculum digitale.

“La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell’informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: “l’uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet”. Il Curricolo della scuola del primo ciclo di istruzione sulle competenze digitali per gli alunni è trasversale alle discipline previste dalle Indicazioni Nazionali: la competenza digitale è ritenuta dall’Unione Europea competenza chiave, per la sua importanza e pervasività nel mondo d’oggi. L’approccio per discipline scelto dalle Indicazioni non consente di declinarla con le stesse modalità con cui si possono declinare le competenze chiave nelle quali trovano riferimento le discipline formalizzate. Si ritrovano abilità e conoscenze che fanno capo alla competenza digitale in tutte le discipline e tutte concorrono a costruirla. Competenza digitale significa padroneggiare certamente le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto

utilizzarle 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.

Le competenze digitali richiamano diverse dimensioni sulle quali sarà possibile lavorare in classe, in un'ottica che integra la dimensione tecnologica con quella cognitiva ed etica:

- dimensione tecnologica: è importante far riflettere i più giovani sul potenziale delle tecnologie digitali come strumenti per la risoluzione dei problemi della vita quotidiana;
- dimensione cognitiva: fa riferimento alla capacità di creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità;
- dimensione etica e sociale: la prima fa riferimento alla capacità di gestire in modo sicuro i propri dati personali e quelli altrui, e di usare le tecnologie digitali per scopi eticamente accettabili e nel rispetto degli altri. La seconda, invece, pone l'accento sulle pratiche sociali.

Nel dettaglio si allega programmazione come presente agli atti:

OBIETTIVI PER LE COMPETENZE DIGITALI (CLASSE 1)

Risolvere i problemi

-Conoscere ed utilizzare in modo appropriato pc/tablet: mettere in atto le procedure corrette (accensione, avvio di programmi e spegnimento);

-Utilizzare programmi

(Paint, Word,...).

-Utilizzare PC/tablet e l.i.m. per eseguire semplici giochi didattici.

-Creazione di contenuti digitali

-Programmare percorsi con l'uso di indicatori spaziali (es. carte CodyRoby)

-Realizzare immagini su reticoli (pixel-art)

-Realizzare percorsi con Bee Bot

-Programmare percorsi di livelli progressivi sulla piattaforma code.org

Alfabetizzazione su informazioni e dati

-Ricerca dati (utilizzando motori di ricerca Chrome, Explorer, Mozilla.....)

Comunicazione e collaborazione

-Utilizzare strumenti e strategie di condivisione e collaborazione;

OBIETTIVI PER LE COMPETENZE DIGITALI (CLASSI 2)

Risolvere i problemi

- Utilizzare in modo appropriato pc/tablet: - mettere in atto le procedure corrette (accensione, avvio di programmi e spegnimento);

-utilizzare programmi (Paint, Open Office,.).

-Utilizzare PC/tablet e l.i.m. per eseguire semplici giochi didattici.

- Creazione di contenuti digitali
 - Programmare percorsi con l'uso di indicatori spaziali (es. carte CodyRoby) e successioni di azioni (CodyWay, diagrammi di flusso...)
 - Realizzare immagini su reticoli (pixel-art)
 - Realizzare percorsi con Bee Bot
 - Programmare percorsi di livelli progressivi sulla piattaforma code.org
- Alfabetizzazione su informazioni e dati
 - Ricercare dati (utilizzando motori di ricerca Chrome, Explorer, Mozilla.)
- Comunicazione e collaborazione
 - Utilizzare strumenti e strategie di condivisione e collaborazione);

OBIETTIVI PER LE COMPETENZE DIGITALI (CLASSE 3)

Risolvere i problemi

- Utilizzare in modo appropriato pc/tablet: - utilizzare programmi (Open Office, foglio di testo, presentazione.);
- mettere in atto le procedure corrette (creazione / salvataggio file,immagini e cartelle);
- Utilizzare PC/tablet e l.i.m. per eseguire semplici giochi didattici.

Creazione di contenuti digitali

- Programmare percorsi (es. carte CodyRoby, CodyWay, diagrammi di flusso.);
 - Realizzare immagini su reticoli (pixel-art);
 - Programmare per livelli progressivi sulla piattaforma Code.org,
- Alfabetizzazione su informazioni e dati
- Ricercare dati (utilizzando motori di ricerca Chrome, Explorer, Mozilla.....)

Comunicazione e collaborazione

- Utilizzare strumenti e strategie di condivisione e collaborazione);

Sicurezza

- Utilizzare in modo consapevole la rete, adottare comportamenti che proteggano e tutelino l'identità digitale propria ed altrui (privacy, password, copyright, cyberbullismo...

OBIETTIVI PER LE COMPETENZE DIGITALI (CLASSE 4)

Risolvere i problemi

- Utilizzare in modo appropriato pc/tablet:- utilizzare programmi (Open Office, foglio di testo, tabella, presentazione.); - mettere in atto le procedure corrette (creazione /salvataggio file, immagini e cartelle)
- Utilizzare PC/tablet e l.i.m. per eseguire semplici giochi didattici.

Creazione di contenuti digitali

- Realizzare immagini su reticoli (pixel-art)
- Programmare per livelli progressivi sulla piattaforma code.org

- Programmare per livelli progressivi strumenti di robotica (Bee-bot, LegoWedo, Ozobot,...)
- Programmare e creare sequenze animate (Scratch)
- Organizzare dati e informazioni per realizzare mappe concettuali, linee del tempo, schemi, diagrammi, quiz....(es. Popplet, Thinglink, Kahoot,Padlet, ...);
- Alfabetizzazione su informazioni e dati
- Ricerca dati (utilizzando motori di ricerca Chrome, Explorer,Mozilla....)
- Comunicazione e collaborazione
- Utilizzare strumenti e strategie di condivisione e collaborazione);
- Sicurezza
- Utilizzare in modo consapevole la rete, adottare comportamenti che proteggano e tutelino l'identità digitale propria ed altrui (privacy, password, copyright, cyberbullismo.)

OBIETTIVI PER LE COMPETENZE DIGITALI (CLASSI 5)

Risolvere i problemi

- Utilizzare in modo appropriato pc/tablet: - utilizzare programmi (Open Office, foglio di testo, tabella, presentazione, foglio elettronico e grafici.);
- mettere in atto le procedure corrette (creazione / salvataggio file, immagini e cartelle);
- Utilizzare PC/tablet e l.i.m. per eseguire semplici giochi didattici.

Creazione di contenuti digitali

- Realizzare immagini su reticoli (pixel-art)
- Programmare per livelli progressivi sulla piattaforma Code.org,
- Programmare per livelli progressivi strumenti di robotica (Bee-bot, Lego Wedo, Ozobot.);
- Costruire circuiti elettrici utilizzando pile, led, motorini, buzzer e blocchi elettronici (schede Arduino);
- Programmare e creare sequenze animate (Scratch);
- Organizzare dati e informazioni per realizzare mappe concettuali, linee del tempo, schemi, diagrammi, quiz....(es. Popplet, Thinglink, Kahoot, Padlet,.....);
- Alfabetizzazione su informazioni e dati
- Ricerca dati (utilizzando motori di ricerca Chrome, Explorer, Mozilla.)

Comunicazione e collaborazione

- Utilizzare strumenti e strategie di condivisione e collaborazione);

Sicurezza

- Utilizzare in modo consapevole la rete, adottare comportamenti che proteggano e tutelino l'identità digitale propria ed altrui (privacy,password, copyright, cyberbullismo...

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 corpo docente ha partecipato a corsi di formazione anche nell'ambito di piani nazionali, oltre che ad iniziative organizzate dall'istituzione o dalle scuole associate in rete e possiede generalmente una buona base di competenze e nel caso delle figure di sistema, anche di carattere specialistico. E' inoltre disponibile ad aggiornarsi per mantenere al passo la propria formazione.

Il percorso complesso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica, non esauribile nell'arco di un anno scolastico, può pertanto prevedere momenti di auto-aggiornamento, momenti di formazione personale o collettiva anche all'interno dell'istituto, con la condivisione delle conoscenze dei singoli e il supporto dell'Animatore digitale, la partecipazione alle iniziative promosse dall'Amministrazione centrale e dalle scuole polo; può comprendere altresì la fruizione dei materiali messi a disposizione dall'Animatore digitale stesso sulle bacheche virtuali appositamente create, corsi di aggiornamento online.

Fondamentale che vi sia attenzione all'uso delle TIC nella didattica: un loro utilizzo strutturato e integrato non solo può rendere gli apprendimenti motivanti, coinvolgenti ed inclusivi, ma permette al docente di guidare studenti e studentesse rispetto alla fruizione dei contenuti online, ormai la modalità naturale di apprendimento al di fuori della scuola. Inoltre, permettono di sviluppare capacità che sono più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza e il confronto fra pari in modalità asincrona.

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.

Anche il percorso della formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet, può prevedere momenti di auto-aggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi. Sarà predisposta una bacheca online per la messa a disposizione e la condivisione di materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di internet, collegata alla homepage del sito scolastico. Qui è possibile trovare materiali informativi sulla sicurezza in internet per l'approfondimento personale, per le attività con gli studenti e gli incontri con i genitori.

Si potrebbe anche pensare ad un cronoprogramma che consideri il triennio scolastico, in un'ottica di vera e propria programmazione, con azioni specifiche.

Per esempio:

1. analizzare il fabbisogno formativo degli insegnanti sull'uso sicuro della rete;
2. promuovere la partecipazione dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto "Generazioni Connesse";
3. monitorare le azioni svolte per mezzo di specifici momenti di valutazione;
4. organizzare incontri con professionisti della scuola o con esperti esterni, enti/associazioni, etc.

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.

L'Istituto attiverà iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine sono previsti incontri fra docenti e genitori per la diffusione del materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati e dalle Forze dell'ordine. Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo. Sul sito scolastico saranno messi in condivisione materiali dedicati agli alunni e alle famiglie come guide in formato pdf e video che possono fornire spunti di approfondimento e confronto.

Il nostro piano d'azioni

Azioni da sviluppare entro un'annualità scolastica.

- 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.

Azioni da svolgere nei prossimi 3 anni

- 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.

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.

Il personale scolastico è incaricato del trattamento dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessari, ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Tutto il personale incaricato riceve istruzioni particolareggiate, applicabili al trattamento di dati personali su supporto cartaceo e informatico, ai fini della protezione e sicurezza degli stessi. I dati personali sono protetti secondo la normativa vigente. Viene richiesta specifica autorizzazione per l'utilizzo di foto, video, testi per la documentazione di attività didattiche, anche in occasione di eventi o manifestazioni e per la pubblicazione sul sito della scuola, social e altri canali (facebook)

E' importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali che si trovano a trattare, in particolare quando sono coinvolti soggetti minorenni. Il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Tutto il personale incaricato riceve poi istruzioni particolareggiate applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi. Anche la diffusione sempre maggiore di smartphone tra i preadolescenti, l'uso di tablet a scopo didattico, la condivisione online di contenuti didattici, l'uso del registro elettronico, l'accesso a piattaforme di videoconferenza, l'eventualità di gruppi whatsapp tra genitori e docenti obbliga la scuola ad avere un'attenzione particolare non solo alla privacy in generale, ma anche alla gestione della privacy legata all'uso dei nuovi dispositivi. La velocità, l'immediatezza con cui si risponde ai messaggi o si condividono foto o video, può far perdere il controllo di dati personali e mettere a rischio la reputazione e la sicurezza dei soggetti coinvolti.

L'istituzione scolastica, durante lo svolgimento dei suoi compiti, rispetta la privacy attraverso il corretto trattamento dei dati personali, presupposto necessario per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza.

La scuola ha l'obbligo:

1. di informare (tramite apposita informativa) gli interessati delle caratteristiche e modalità del trattamento dei loro dati;
2. di chiedere il consenso informato per il trattamento dei dati personali;
3. di trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali;
4. di redigere e mantenere un registro del trattamento dei dati, sia per il titolare che per il responsabile del trattamento;

5. di adottare idonee misure tecniche e organizzative per garantire il diritto alla riservatezza e la sicurezza dei trattamenti

Sul sito del nostro istituto è possibile visionare le liberatorie adottate nel totale rispetto della privacy

<https://www.aldomorocd.edu.it/>

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.

Disposizioni sull'accesso ad internet

- l'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico, di formazione, amministrativo;
- ciascun utente è personalmente responsabile per l'uso del proprio account ed è tenuto a tutelarlo da accessi non autorizzati;
- la password del registro elettronico è personale e riservata, pertanto è vietato l'uso della password di altri utenti. Qualora se ne venisse a conoscenza è obbligatorio segnalare il fatto all'utente interessato o al docente responsabile;
- Internet non può essere usato per scopi vietati dalla legislazione vigente;
- l'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso improprio del servizio Internet;
- è vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza;

Gestione accessi (password, backup, filtri ecc.)

- l'uso dei dispositivi da parte degli alunni è permesso soltanto su autorizzazione dell'insegnante;
- ogni docente e ogni genitore accede al Registro Elettronico attraverso una password personale che non può essere comunicata a terzi .
- il sito web della scuola è gestito, implementato e tempestivamente aggiornato dal docente Funzione Strumentale; la Segreteria si occupa della pubblicazione dei contenuti più strettamente amministrativi. Il Dirigente scolastico controlla e autorizza i contenuti e le informazioni pubblicate.

Il regolamento, dunque, deve prevedere una parte dedicata all'uso di Internet in cui gli studenti si impegnano a:

- utilizzare la rete nel modo corretto;
- rispettare le consegne dei docenti;
- non scaricare materiali e software senza autorizzazione;
- non utilizzare unità rimovibili personali senza autorizzazione;
- tenere spento i dispositivi al di fuori delle attività didattiche che ne prevedano l'utilizzo;
- durante le attività che prevedono l'utilizzo di dispositivi informatici, utilizzarli esclusivamente per svolgere le attività didattiche previste;
- segnalare immediatamente materiali inadeguati ai propri insegnanti.

I docenti si impegnano a:

- utilizzare la rete nel modo corretto;
- non utilizzare device personali se non per uso didattico;

- formare gli studenti all'uso della rete;
- dare consegne chiare e definire gli obiettivi delle attività;
- monitorare l'uso che gli studenti fanno delle tecnologie a scuola.

Checklist

- mantenere separate le reti didattica e segreteria;
- aggiornare periodicamente software e sistema operativo;
- definire la programmazione di backup periodici;
- garantire formazione adeguata allo staff, incluso il corpo docenti;
- testare regolarmente le possibili vulnerabilità;
- preparare piani di azione in risposta ai problemi più seri;
- predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo;
- impostare il browser per l'eliminazione dei cookies alla chiusura.

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.

Grazie all'uso delle tecnologie digitali, da una comunicazione uno a molti, si può passare ad una comunicazione che per definizione può essere molti a molti, multimediale, bidirezionale e interattiva.

Ciò naturalmente può rappresentare un'opportunità significativa anche in termini di un maggiore coinvolgimento degli studenti o dei genitori, o alla possibilità di usare diversi linguaggi (scrittura, immagini, video etc.) ma in taluni casi può anche rivelarsi un problema non sempre facile da gestire. Si pensi, ad esempio, all'uso talvolta smodato e senza regole che docenti, ragazzi o genitori fanno dei gruppi whatsapp. In riferimento all'uso degli strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne, come avviene generalmente tra i docenti

mediante, ad esempio l'uso di gruppi telegram o whatsapp, è importante ricordare quello che si può definire "diritto alla disconnessione".

L'art. 22 (Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola) del CCNL 2016/2018, infatti, fa riferimento ai criteri generali per l'utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio, al fine di una maggiore conciliazione tra vita lavorativa e vita familiare. È importante sottolineare però che per le chat informali tra colleghi, o tra docenti e genitori, non esiste una vera e propria regolamentazione, e per tale ragione è fondamentale, a partire dal buon senso e da una riflessione sulle peculiarità del mezzo, che si elaborino regole condivise sull'uso delle stesse.

Fra queste, ad esempio, ipotizziamo:

- comprendere e rispettare sempre le finalità del gruppo, scrivendo e pubblicando solo contenuti pertinenti a tali finalità;
- usare sempre un linguaggio adeguato e il più possibile chiaro e preciso;
- evitare di affrontare in chat argomenti troppo complessi e controversi (che certamente è più opportuno affrontare in presenza o in un Consiglio di classe);
- evitare discussioni di questioni che coinvolgono due o pochi interlocutori, onde evitare di annoiare e disturbare gli altri componenti del gruppo;
- non condividere file multimediali troppo pesanti;
- evitare il più possibile di condividere foto di studenti in chat;
- indirizzare solo domande precise e chiare, a cui si possano dare risposte altrettanto brevi e precise;
- evitare messaggi troppo spezzettati, cercando il più possibile di essere brevi ed esaustivi allo stesso tempo.

3.4 - Strumentazione personale

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.

In tal senso, dispositivi personali possono essere integrati nell'attività didattica quando ben progettata e calibrata per discipline e obiettivi formativi e didattici.

Di seguito, i dieci punti del Miur per l'uso dei dispositivi mobili a scuola, BYOD (Bring your own device):

1. Ogni novità comporta cambiamenti. Ogni cambiamento deve servire per migliorare l'apprendimento e il benessere delle studentesse e degli studenti e più in generale dell'intera comunità scolastica.
2. I cambiamenti non vanno rifiutati, ma compresi e utilizzati per il raggiungimento dei propri scopi. Bisogna insegnare a usare bene e integrare nella didattica quotidiana i dispositivi, anche attraverso una loro regolamentazione. Proibire l'uso dei dispositivi a scuola non è la soluzione. A questo proposito ogni scuola adotta una Politica d'Uso Accettabile (PUA) delle tecnologie digitali.
3. La scuola promuove le condizioni strutturali per l'uso delle tecnologie digitali. Fornisce, per quanto possibile, i necessari servizi e l'indispensabile connettività, favorendo un uso responsabile dei dispositivi personali (BYOD). Le tecnologie digitali sono uno dei modi per sostenere il rinnovamento della scuola.
4. La scuola accoglie e promuove lo sviluppo del digitale nella didattica. La presenza delle tecnologie digitali costituisce una sfida e un'opportunità per la didattica e per la cultura scolastica. Dirigenti e insegnanti attivi in questi campi sono il motore dell'innovazione. Occorre coinvolgere l'intera comunità scolastica anche attraverso la formazione e lo sviluppo professionale.
5. I dispositivi devono essere un mezzo, non un fine. È la didattica che guida l'uso competente e responsabile dei dispositivi. Non basta sviluppare le abilità tecniche, ma occorre sostenere lo sviluppo di una capacità critica e creativa.
6. L'uso dei dispositivi promuove l'autonomia delle studentesse e degli studenti. È in atto una graduale transizione verso situazioni di apprendimento che valorizzano lo spirito d'iniziativa e la responsabilità di studentesse e gli studenti. Bisogna sostenere un approccio consapevole al digitale nonché la capacità d'uso critico delle fonti di informazione, anche in vista di un apprendimento lungo tutto l'arco della vita.
7. Il digitale nella didattica è una scelta: sta ai docenti introdurla e condurla in classe. L'uso dei dispositivi in aula, siano essi analogici o digitali, è promosso dai docenti, nei modi e nei tempi che ritengono più opportuni.
8. Il digitale trasforma gli ambienti di apprendimento. Le possibilità di apprendere sono ampliate, sia per la frequentazione di ambienti digitali e condivisi, sia per l'accesso alle informazioni, e grazie alla connessione continua con la classe. Occorre regolamentare le modalità e i tempi dell'uso e del non uso, anche per imparare a riconoscere e a mantenere separate le dimensioni del privato e del pubblico.
9. Rafforzare la comunità scolastica e l'alleanza educativa con le famiglie. È necessario

che l'alleanza educativa tra scuola e famiglia si estenda alle questioni relative all'uso dei dispositivi personali. Le tecnologie digitali devono essere funzionali a questa collaborazione. Lo scopo condiviso è promuovere la crescita di cittadini autonomi e responsabili.

10. Educare alla cittadinanza digitale è un dovere per la scuola. Formare i futuri cittadini della società della conoscenza significa educare alla partecipazione responsabile, all'uso critico delle tecnologie, alla consapevolezza e alla costruzione delle proprie competenze in un mondo sempre più connesso.

Il nostro piano d'azioni

Azioni da sviluppare entro un'annualità scolastica:

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

Azioni da sviluppare nei prossimi 3 anni.

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

Se le Tecnologie dell'Informazione e della Comunicazione (TIC) sono parte integrante della vita quotidiana dei più giovani, in quanto strumenti privilegiati di comunicazione e di relazione, ma anche di informazione, studio, creatività e partecipazione, esse pongono però delle questioni associate alla "sicurezza" e al comportamento sociale.

I rischi online rappresentano tutte quelle situazioni problematiche derivanti da un uso

non consapevole e non responsabile delle tecnologie digitali da parte di bambini/e, ragazzi e ragazze: adescamento online, cyberbullismo, sexting, violazione della privacy, pornografia (recenti ricerche hanno sottolineato come la maggior parte degli adolescenti reperisca in Rete informazioni inerenti la sessualità, col rischio, spesso effettivo, del diffondersi di informazioni scorrette e/o l'avvalorarsi di falsi miti), pedopornografia (con questo termine si intende qualsiasi foto o video di natura sessuale che ritrae persone minorenni), gioco d'azzardo o gambling, internet addiction, videogiochi online (alcuni rischi associati possono essere ad esempio: contatti impropri con adulti, contenuti violenti e/o inadeguati; acquisti incontrollati, etc.), esposizione a contenuti dannosi o inadeguati (es. contenuti razzisti, che inneggiano al suicidio, che promuovono comportamenti alimentari scorretti, etc.), etc. Partendo da questo punto di vista, vanno promosse nei più giovani le necessarie competenze e capacità, al fine di una protezione adeguata, ma anche al fine di un utilizzo consapevole che sappia sfruttare le potenzialità delle tecnologie digitali e gestirne le implicazioni.

Il nostro Istituto intende sensibilizzare e prevenire il fenomeno crescente dei rischi online attraverso una serie di interventi, agendo su più livelli:

1. a livello di comunità locale, in un'ottica di psicologia di comunità; ricerca-azione e di lavoro in rete;
2. a livello di comunità scolastica, attraverso la cooperazione tra scuola e famiglia e l'elaborazione di una programmazione educativo-didattica contro i rischi online;
3. a livello del gruppo classe, con un approccio curricolare teso:

-al potenziamento delle abilità sociali;
-alla promozione della cooperazione;
-alla mediazione del conflitto tra i pari;

4. a livello del singolo, con il sostegno individuale e il supporto in classe attraverso vari approcci:

-l'approccio umanistico che si basa sulla capacità di ascoltare e di stabilire una sana comunicazione, per aiutare a sviluppare gradualmente la capacità empatica;
-l'approccio morale che si fonda sulla riflessione come opportunità per interiorizzare le regole della comunità;
-l'approccio disciplinare che comprende la conoscenza di regole condivise, regolamenti, leggi e l'applicazione di una punizione o pena che può essere da lieve a severa in base alla gravità.

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).

CYBERBULLISMO

Per «cyberbullismo» si intende 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.(1)

L'avvento di Internet ha creato indubbiamente nuovo spazio per i processi di

socializzazione degli adolescenti che, attraverso di esso, possono esprimersi in un contesto in cui i confini tra realtà virtuale e vita reale risultano non sempre definibili.

Sebbene internet per molti ragazzi rappresenti un utile strumento di studio e di ricerca, purtroppo si deve registrare la crescente tendenza verso un uso negativo delle sue potenzialità attraverso l'invio di messaggi insolenti o minacciosi tramite e-mail o chat, commenti denigratori sul conto della vittima e minacce fisiche online, filmati e fotografie umilianti sulle vittime diffusi in rete.

Tutte queste forme di attacco sono ripetute nel tempo e sono fatte intenzionalmente per colpire la vittima usando una forma di "bullismo" che in questo caso, rispetto al bullismo tradizionale, si manifesta attraverso la capacità di usare i nuovi mezzi tecnologici in modo rapido e anonimo.

Il fenomeno generale del bullismo ha assunto perciò nuove forme tutte riconducibili all'espressione inglese "cyberbullying" (bullismo elettronico) che indica appunto l'utilizzo di informazioni elettroniche e dispositivi di comunicazione come e-mail, sms, blogs, siti web, telefoni cellulari per molestare in qualche modo una persona o un gruppo, attraverso attacchi personali talora di criminosa gravità tale da rovinare letteralmente la vita delle vittime.

Particolarmente preoccupante è la pratica definita "**happy slapping**", cioè la ripresa (spesso effettuata senza permesso) da parte del persecutore di immagini strettamente private e imbarazzanti al fine di diffamare (come nel cosiddetto **sexting**), ricattare e "punire" la persona protagonista del video, per allontanarla dal gruppo di appartenenza o per vendicarsi di qualche rifiuto o sgarbo.

Tale punizione avviene con la pratica denominata "**kick**" (cioè "calcio") e il modo preferito dai *cyberstalkers* è quello di inserire oltre al filmato imbarazzante della loro vittima anche il numero di telefono accompagnato dall'invito a contattarla per ricevere prestazioni sessuali.

Purtroppo, si sono già avuti casi di suicidio da parte alcune vittime sconvolte dall'umiliazione e dalla vergogna.

Per riassumere, il **cyberbullismo**, possiede una serie di caratteristiche specifiche:

- **Pervasività:** se il bullo tradizionale si ferma fuori la porta di casa, il cyberbullo è sempre presente sulle varie tecnologie usate (sms, WhatsApp, Facebook, internet, YouTube, Instagram, ecc.).
- **Anonimato:** dà ai bulli la sensazione percepita di rimanere anonimi.
- **Volontarietà dell'aggressione:** non sempre gli effetti negativi sono provocati da un'azione mirata; non potendo osservare le reazioni della vittima, si commettono atti persecutori non comprendendo che ci si è spinti troppo oltre.
- **Ampiezza di portata:** i messaggi e i materiali inviati sono trasmessi, ritrasmessi e amplificati oltre la cerchia dei conoscenti.

Atteggiamento tipico di difesa del bullo e del cyberbullo è l'**attivazione di meccanismi di disimpegno morale**.

Le strategie di disimpegno morale che più facilmente possono venire adottate dai bulli/cyberbulli una volta scoperti sono le seguenti:

- **Minimizzazione:** gli atti che si sono compiuti sono considerati “solo uno scherzo”.
- **Diffusione della responsabilità:** “Non è colpa mia. Lo facevano tutti” oppure “Io non ho fatto niente, ho solo postato un messaggio che mi era arrivato”.
- **Distorsione delle conseguenze:** “Non credevo se la prendesse, lo sa che scherziamo”, in quanto far del male a una persona risulta più facile se la sua sofferenza è nascosta.
- **Attribuzione della colpa:** spostarla da sé e addossandola all’altro “ha iniziato lui” “è lei che si è spogliata” ecc.

Rientrano nel **CYBERBULLISMO**:

- **Flaming:** Litigi on line nei quali si fa uso di un linguaggio violento e volgare.
- **Harassment:** molestie attuate attraverso l’invio ripetuto di linguaggi offensivi.
- **Cyberstalking:** invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la propria incolumità.
- **Denigrazione:** pubblicazione all’interno di comunità virtuali, quali newsgroup, blog, forum di discussione, messaggistica immediata, siti internet...di pettegolezzi e commenti crudeli, calunniosi e denigratori.
- **Outing estorto:** registrazione delle confidenze - raccolte all’interno di un ambiente privato- creando un clima di fiducia e poi inserite integralmente in un blog pubblico.
- **Impersonificazione:** insinuazione all’interno dell’account di un’altra persona con l’obiettivo di inviare dai medesimi messaggi ingiuriosi che screditino la vittima.
- **Esclusione:** estromissione intenzionale dall’attività on line.
- **Sexting:** invio di messaggi via smartphone ed Internet, corredati da immagini a sfondo sessuale.

Gli interventi di prevenzione, formazione e presa in carico devono avvenire su diversi livelli: con la comunità scolastica, con il gruppo classe, e con il singolo.

Si prevedono nel corso del triennio:

-Attività informativa e di sensibilizzazione rivolta a ragazzi, genitori, insegnanti e personale scolastico, per favorire la conoscenza e la comprensione del fenomeno del bullismo e del cyberbullismo;

-Incontri di formazione, incontri/dibattito tenuti da esperti (psicologi, sociologi, Polizia postale, giudici del Tribunale dei minori, referenti associazione genitori, Enti del territorio), per alunni, docenti, genitori al fine di far conoscere il fenomeno delle devianze, gli strumenti di comunicazione/interazione in Internet, i possibili rischi della rete;

-Confronto con le figure istituzionali di riferimento, cui ognuno potrà rivolgersi ogniqualvolta lo ritenga necessario.

-Interventi a livello di classe che prevedono la partecipazione attiva ed esperienziale degli studenti. A questo livello si può lavorare con i bambini su quelle conoscenze e competenze che gli studi hanno dimostrato essere alla base del fenomeno del bullismo, attraverso:

1. attività per sollecitare la capacità di riconoscere le proprie emozioni e quelle degli altri;
2. attività per favorire la conoscenza di sé stessi, dei propri punti di forza e di debolezza e il pensiero assertivo;
3. attività finalizzate alla capacità di comunicare con gli altri con sicurezza ed efficacia, incrementando le proprie abilità interpersonali;
4. visione di filmati, spot, cortometraggi sul tema; discussione guidata, letture tematiche.

Si prevede l'utilizzo di metodi di insegnamento interattivi, incentrati sulle life skills e sul modello socio-affettivo per favorire nei bambini l'acquisizione delle abilità e delle competenze di vita.

(1) Cfr. Legge 29 maggio 2017 n.71 articolo 1comma2

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.

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

Il contenuto e il tono

Certe espressioni di odio sono più estreme, utilizzano termini più insultanti e possono perfino istigare altri ad agire. All’altra estremità della scala, troviamo insulti più moderati o generalizzazioni eccessive, che presentano certi gruppi o individui sotto una cattiva (e perfino sotto falsa) luce. L’intenzione degli autori degli insulti Ci può capitare di offendere gli altri senza volerlo, e poi di pentircene, e perfino di ritirare quanto abbiamo detto. Nei due esempi seguenti, entrambe le affermazioni sono intolleranti e sgradevoli, ma una è stata scritta con l’intenzione di offendere e fare del male.

I bersagli o i bersagli potenziali

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

Il contesto

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

L'impatto reale o l'impatto potenziale

L'impatto reale o potenziale esercitato sugli individui, sui gruppi o sull'insieme della società è una delle principali considerazioni da tenere presenti. Spesso, le ripercussioni negative subite dall'individuo o dal gruppo si rivelano più importanti della valutazione dell'episodio da parte di osservatori esterni. Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono quindi un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete.

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

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?

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

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

- la ricerca di equilibrio nelle relazioni anche online;
- l'uso degli strumenti digitali per il raggiungimento di obiettivi personali;
- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile;
- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche).

Questo è un argomento trasversale, se ne può parlare quando si parla di cittadinanza digitale, di cyberbullismo, di uso integrativo non sostitutivo dei dispositivi e della Rete; tanto più può essere utile dedicare al tema un momento specifico e riflettere con studenti e studentesse per fare in modo che la tecnologia sia strumento per

raggiungere i propri obiettivi e non sia solo distrazione o addirittura ostacolo.

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.

Strutturare regole condivise e stipulare con gli studenti una sorta di "patto" d'aula e, infine, proporre delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d'aula (Es. adoperando la LIM o il dispositivo personale. Si veda il BYOD di cui abbiamo parlato nel precedente modulo). È importante, quindi, non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli/le studentie delle studentesse, stabilendo chiare e semplici regole di utilizzo.

Il ruolo della formazione è particolarmente rilevante per poter osservare ed accogliere le richieste di aiuto dei minori. Attraverso la rete di servizi integrata, gli insegnanti devono essere formati rispetto alle dipendenze patologiche per poter individuare i segnali di allarme nei comportamenti degli studenti. Grazie alla formazione saranno in grado di fornire informazioni corrette e di progettare interventi di prevenzione efficaci nella scuola, anche in collaborazione con altri esperti.

La nostra scuola intende attivare azioni di prevenzione tenendo conto dell'età di riferimento: la fascia d'età che massimizza l'efficacia degli interventi è la scuola secondaria di primo grado.

Le azioni educativo -didattiche prevedono:

- trattazione, anche con esperti esterni, di tematiche rilevanti e coerenti con la loro esperienza quotidiana;

- approcci inclusivi che valorizzino le capacità degli alunni (ad esempio sfruttare le potenzialità di tecnologie hardware e software appositamente progettate per il contesto educativo (robot educativi, coding). Percorsi di questo genere diventano "palestre" dove i ragazzi rafforzano le relazioni sociali necessarie per il loro benessere emotivo e si allenano a cooperare in team; imparano ad accettare la frustrazione generata dalle difficoltà e dall'errore, sviluppano funzioni cognitive superiori necessarie anche per l'auto-controllo e la presa di decisione);

- sviluppo delle competenze di vita;

- osservazione sistematica da parte dei docenti dei sintomi comportamentali e cognitivi (disturbi di attenzione, iperattività, scarso rendimento scolastico, perdita di interesse verso altre passioni, ansia, isolamento, aggressività, uso di sostanze);

- Incontri di formazione con esperti, rivolti ai genitori, per far conoscere fenomeni e contesti con cui vengono a contatto i loro figli. Le famiglie devono sapere chi frequentano i loro ragazzi nella vita reale e in quella virtuale, anche chiedendo il supporto a chi di dovere. Occorrono regole precise sul tempo da trascorrere davanti al pc, sulle fasce orarie consentite e, non ultimo, sui filtri di navigazione.

- Dialogo stretto scuola-famiglia affinché i genitori approfondiscano la conoscenza del fenomeno e attuino una stretta vigilanza rispetto all'uso che si fa delle nuove tecnologie, con il controllo di telefoni, pc o tablet.

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 medialti 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.

La consapevolezza, o comunque la sola idea di diffusione di contenuti personali, si replica nel tempo e può finire con il danneggiare, sia in termini psicologici che sociali, sia il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che hanno contribuito a diffonderla. A ciò si associano altri comportamenti a rischio, di tipo sessuale ma anche riferibili ad abuso di sostanze o di alcool. I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/i e depressione

4.6 - Adescamento online

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

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

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

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

Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere, ad

esempio, all'adescatore. È importante che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove. Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video...).

L'adescamento, inoltre, può essere una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico. I minori vittime di adescamento riferiscono, generalmente, di sentirsi traditi, ma anche di provare un senso di colpa per essere caduti in trappola ed essersi fidati di uno sconosciuto.

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

Per consigli e per un supporto è possibile rivolgersi alla Helpline di Generazioni Connesse (19696):

- operatori esperti e preparati sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che dei bambini, degli adolescenti, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti l'utilizzo dei nuovi media.

4.7 - Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, **concrete o simulate** o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

La legge n. 269 del 3 agosto 1998 *"Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù"*, introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella **legge n. 38 del 6 febbraio 2006** *"Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet"*, segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.)

che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Secondo la Legge 172/2012 - Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione "**Segnala contenuti illegali**" ([Hotline](#)).

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

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. Ad esempio, non è utile diffondere tra i bambini e le bambine più piccoli/e l'uso di servizi come le hotline, sia perché in caso di visione accidentale di materiale pedopornografico è opportuno che bambini/e e ragazzi/e possano parlarne con gli adulti di riferimento per la migliore risposta possibile, sia perché si potrebbe incentivare la ricerca proattiva, che comunque è vietata dalla legge italiana, per minori e per adulti.

Risulta utilissima l'attività educativa sull'affettività e le relazioni, sottolineando sempre la necessità di rivolgersi ad un adulto quando qualcosa online mette a disagio. 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 delle hotline.

Il nostro piano d'azioni

Azioni da sviluppare entro un'annualità scolastica:

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

Azioni da sviluppare nei prossimi 3 anni.

- 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.
- 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.

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.

Risulta fondamentale imparare a riconoscere i rischi più comuni che i bambini e gli adolescenti possono correre navigando sul web, per poter intervenire in modo adeguato ed efficace prima che la situazione diventi più grave e compromettente.

I bambini e i preadolescenti possono imbattersi in materiale non autorizzato, messaggi offensivi e minacciosi, immagini violente e imbarazzanti, contenuti pericolosi o ancora richieste di sesso online e pedopornografia. Esperienze e situazioni che possono influenzare e segnare profondamente un ragazzo nella crescita e nei suoi atteggiamenti futuri.

Devono pertanto essere segnalati:

- link sospetti o siti non protetti che fanno richieste indebite o ingiustificate
- uso inappropriato di documenti, audio e video coperti dal diritto d'autore
- siti che diffondono disinformazione
- contenuti inappropriati afferenti all'aggressività, alla violenza, alla discriminazione, all'odio, alla sfera sessuale
- contenuti che violano la privacy
- profili falsi e malevoli

Genitori, educatori ed insegnanti devono prestare particolare attenzione, attraverso l'osservazione e il dialogo, ai sintomi e ai segnali che i minori possono manifestare:

- senso di malessere, agitazione, insonnia
- comportamenti compulsivi o ossessivi (controllo ripetuto del telefono, prolungati periodi in chat, dipendenza)
- scarso profitto, assenteismo scolastico, isolamento sociale anche totale
- cambiamenti drastici dello stile di vita, nell'alimentazione e riduzione dell'attività fisica o delle attività extrascolastiche
- comportamenti regressivi
- riluttanza a condividere ciò che fanno
- insicurezza eccessiva ed esplosioni di rabbia inspiegabili
- paura inspiegabile di frequentare la scuola o frequentare determinati luoghi o persone
- comportamenti autolesivi
- precoce e impropria sessualizzazione nei bambini più piccoli

Tutte le misure di prevenzione ai fenomeni oggetto del presente documento sono integrate nel curriculum dei temi trasversali legati al corretto utilizzo delle TIC e della rete Internet: l'eventuale progettazione di unità o progetti didattici specifici potrà essere oggetto di pianificazione a livello di Dipartimenti Disciplinari, comunque andranno calibrati in base all'età degli alunni e alle esigenze reali di ogni classe.

In alcuni casi specifici gli insegnanti, anche con l'ausilio tecnico dell'Animatore digitale e del Referente per il Bullismo, possono provvedere a conservare le prove della condotta incauta, scorretta o dell'abuso rilevati anche sui device della scuola: soprattutto la data e l'ora, il contenuto dei messaggi e, se possibile, l'ID del mittente (es. username, mail, numero di telefono cellulare) o l'indirizzo web del profilo ed il suo

contenuto. Conservare la prova è utile per approfondire sull'accaduto ed informare, accertata la veridicità e la gravità del fatto, il Dirigente scolastico e i genitori degli alunni, e per le condotte illegali le Forze dell'ordine. Nel caso gli illeciti siano avvenuti tramite smartphone o pc di uso personale, possono chiedere ai genitori della presunta vittima prove come testi di messaggio o screenshot come dimostrazione di ciò che viene visualizzato sullo schermo. Nel caso di cellulare ci si può assicurare che l'alunno vittima salvi nel suo telefono ogni messaggio, voce/testo/immagine, conservando così il numero del mittente. Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno/genitore/personale della scuola, quantunque riferite anche a fatti accaduti al di fuori del contesto scolastico, le notizie raccolte sono comunque comunicate al Dirigente scolastico e per fatti rilevanti anche ai genitori. In particolare, la segnalazione viene fatta a entrambe le famiglie, sia della vittima che dell'autore della condotta negativa.

Ogni qualvolta si ha il sospetto o la certezza che uno/a studente/studentessa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ricordatevi, innanzitutto, che nell'affrontare quanto accade non siete mai soli. Siete parte di una comunità scolastica ed è all'interno e con il supporto di essa che il problema va gestito.

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).

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). Nel CASO A, si dovrebbe coinvolgere innanzitutto il referente d'Istituto per il contrasto del bullismo e del cyberbullismo (e/o il referente indicato nell'ePolicy) valutando insieme le possibili strategie d'intervento. Si potrebbe pensare anche alla possibilità di avvisare l'intero consiglio di classe e, se si ravvisa la necessità e l'urgenza, di coinvolgere il Dirigente Scolastico (considerando il regolamento interno o le prassi già consolidate). Nel frattempo, il docente (e i docenti informati) ascolta gli studenti e le studentesse, osservando e monitorando il clima di classe, ciò che accade, le dinamiche relazionali nel contesto classe, senza fare indagini dirette. Uno strumento utile per raccogliere informazioni può essere il diario di bordo. Inoltre, il docente deve cercare di capire se gli episodi sono circoscritti al gruppo o se interessano l'intero Istituto. Operativamente è fondamentale coinvolgere tutti gli studenti e le studentesse, informandoli sui fenomeni e sulle caratteristiche degli stessi, suggerendo di chiedere aiuto se pensano di vivere situazioni, di subire atti identificabili come bullismo o cyberbullismo.

Sarebbe opportuno (sempre monitorando la situazione) prevedere momenti laboratoriali, utilizzando anche la piattaforma Generazioni Connesse nella parte dei contenuti e dei materiali; tali attività possono essere molto positive, stimolare il dialogo e la riflessione fra gli studenti e le studentesse. Infine, sottolineare che è il referente scolastico sulle tematiche che può prendere in carico la situazione, alla luce della normativa vigente e in particolare della Legge n.71 del 2017.

Se avete un dubbio su come procedere o interpretare quello che sta accadendo a scuola, potete richiedere, in qualsiasi momento, una consulenza telefonica alla Helpline del progetto Generazioni Connesse, al numero gratuito [1.96.96](tel:19696).

Se gli agiti osservati si identificano come atti di bullismo o cyberbullismo, il docente e la scuola tutta devono intervenire seguendo il CASO B.

Nel CASO B, il docente deve condividere immediatamente quanto osservato con il referente per il bullismo e il cyberbullismo (e/o il referente indicato nell'ePolicy), valutando insieme le possibili strategie di intervento.

Si avvisa anche il Dirigente Scolastico che convoca il consiglio di classe. Se non si ravvisano fattispecie di reato, si dovrebbe:

- informare i genitori (o chi esercita la responsabilità genitoriale) degli/delle studenti/studentesse direttamente coinvolti/e (qualsiasi ruolo abbiano avuto), se possibile con la presenza dello psicologo, su quanto accade e condividete informazioni e strategie;
- richiedere, in concomitanza, la consulenza dello psicologo scolastico a supporto della gestione della situazione, in base alla gravità dell'accaduto;
- attivare il consiglio di classe;

- valutare come coinvolgere gli operatori scolastici su quello che sta accadendo.

A seconda della situazione e delle valutazioni effettuate con referente, dirigente e genitori, si potrebbe poi segnalare alla Polizia Postale: a) contenuto del materiale online offensivo; b) modalità di diffusione; c) fattispecie di reato eventuale. Se è opportuno, richiedere un sostegno ai servizi e alle associazioni territoriali o ad altre autorità competenti.

È bene sempre dialogare con la classe, attraverso interventi educativi specifici, cercando di sensibilizzare studenti e studentesse sulla necessità di non diffondere ulteriormente online i materiali dannosi, ma anzi di segnalarli e bloccarli. Ciò è utile anche per capire il livello di diffusione dell'episodio all'interno dell'Istituto.

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.

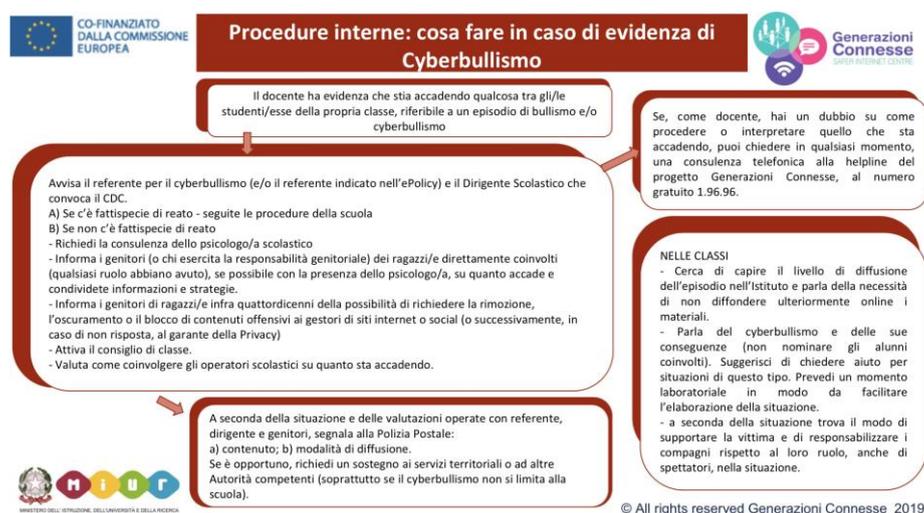
- **Aziende Sanitarie Locali:** forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni 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.

È possibile far riferimento a queste tipologie di uffici:

Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato .

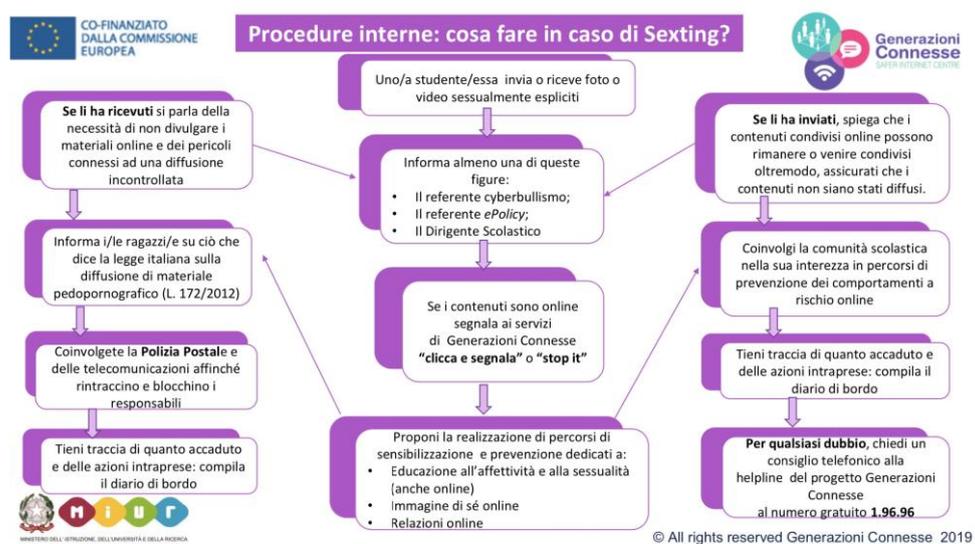
5.4. - Allegati con le procedure

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

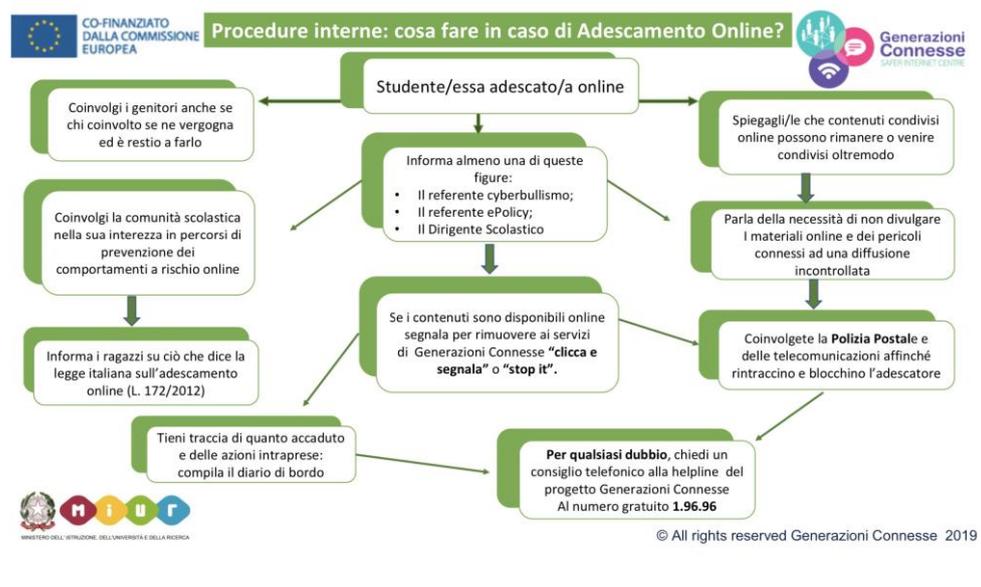




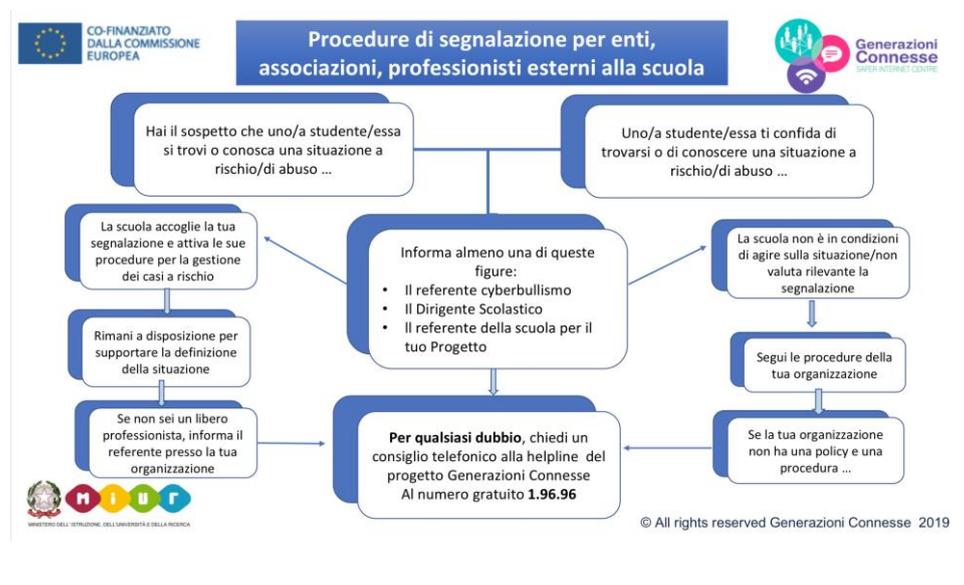
Procedure interne: cosa fare in caso di sexting?



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](#)

Le procedure interne per la rilevazione e la gestione dei casi, nonché la segnalazione

alla Dirigenza Scolastica ed eventualmente alle autorità competenti, avvengono secondo i protocolli suggeriti dalla piattaforma messa a disposizione da "Generazioni Connesse"

Il nostro piano d'azioni

Non è prevista nessuna azione.

