Documento di ePolicy

LEIC89700R

I.C. POLO 2 "RENATA FONTE"

VIA MAURO MANIERI N. 20 - 73048 - NARDO' - LECCE (LE)

Mariagiuditta LEACI

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 curricolo**
    1. Curricolo 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.

Attraverso l'E-policy il nostro Istituto Comprensivo Polo 2 "Renata Fonte" 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 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 ad un uso consapevole delle stesse.
Questa policy si applica a tutti i membri della comunità scolastica che hanno accesso o che sono utenti dei sistemi informatici della scuola. In particolare, essa viene redatta per regolamentare il comportamento degli alunni dentro le aule scolastiche e per sensibilizzarli all'adozione di buone pratiche quando sono fuori dalla scuola. Autorizza i membri del personale docente ad erogare sanzioni disciplinari per comportamenti inappropriati avvenuti all'interno dell'istituzione scolastica. Questo è il caso degli episodi di cyberbullismo come di altri fenomeni di cui si tratta nella presente politica, che possono avvenire al di fuori della scuola, ma che sono legati alla frequenza della stessa. L'I.C. Polo 2 Nardò accoglie minori "nativi digitali" che fin dall'infanzia sono esposti a rischi di cui sono inconsapevoli, pertanto la scuola attua parallelamente attività di prevenzione, controllo e formazione di studenti e famiglie allo scopo di ridurre al minimo l'occorrenza di atti che non solo creano disagio nella comunità scolastica, ma possono configurarsi come reati. La scuola opera in stretto collegamento con le forze dell'ordine, con la Procura della Repubblica, con istituzioni del settore educativo, per mettere in campo strategie di prevenzione al cyber-bullismo e interventi di recupero nel caso in cui vengano individuati tali fenomeni, informando i genitori/tutori e chiedendo la loro collaborazione anche qualora gli episodi si siano verificati al di fuori delle attività didattiche.

Il nostro documento di Policy contiene le misure atte a facilitare e promuovere l'utilizzo positivo delle TIC nella didattica, le misure di prevenzione e di gestione di situazioni problematiche relative all'uso delle tecnologie digitali. Il documento è definito da un insieme di regolamenti, linee di azione e attività poste in essere per fare fronte ad una serie di necessità individuate. Una policy non è mai il risultato di un'azione unica, quanto piuttosto l'esito delle interazioni di un insieme di azioni e decisioni. I suoi contenuti sono:

-misure atte a facilitare e promuovere l'utilizzo delle TIC nella didattica;

-misure di prevenzione;

- misure per la segnalazione e gestione dei casi.

La nostra scuola ha aderito al progetto GENERAZIONI CONNESSE, promosso dal MIUR in collaborazione con la Comunità Europea, ed ha elaborato il presente documento in conformità con le LINEE DI ORIENTAMENTO per

azioni di prevenzione e di contrasto al bullismo e cyberbullismo emanate dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con il Safer Internet Center per l'Italia. Occorre premettere che:

a) il progetto "Generazioni Connesse" è stato inserito nel nostro Piano Triennale dell'Offerta Formativa e le azioni preventivate nel Piano d'Azione della nostra scuola, visto il loro elevato numero e la complessità di alcune di esse, verranno portate avanti progressivamente nei prossimi anni;

b) le attività di promozione all'utilizzo delle tecnologie digitali nella didattica costituiscono un tema centrale per l'attuazione del Piano Nazionale Scuola Digitale e sono già previste nel Piano Triennale dell'Offerta Formativa, in particolare nel progetto predisposto dall'animatore digitale.

1.2 - Ruoli e responsabilità

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

IL DIRIGENTE SCOLASTICO

• individua attraverso il Collegio dei Docenti, un referente del bullismo e cyber bullismo e un'equipe antibullismo da esso coordinata;

• coinvolge, nella prevenzione e contrasto al fenomeno del bullismo, tutte le componenti della comunità scolastica, partendo dall'utilizzo sicuro di Internet a scuola;

• prevede all'interno del PTOF corsi di aggiornamento e formazione in materia di prevenzione dei fenomeni di bullismo e cyberbullismo, rivolti al personale docente e Ata;

• promuove sistematicamente azioni di sensibilizzazione dei fenomeni del bullismo e cyberbullismo nel territorio in rete con enti, associazioni, istituzioni locali ed altre scuole, coinvolgendo alunni, docenti, genitori ed esperti;

• 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;

• prevede azioni culturali ed educative rivolte agli studenti, per acquisire le competenze necessarie all'esercizio di una cittadinanza digitale consapevole.

IL REFERENTE DEL "BULLISMO E CYBERBULLISMO":

• promuove la conoscenza e la consapevolezza del bullismo e del cyber-bullismo attraverso progetti d'Istituto che coinvolgano genitori, studenti e tutto il personale;

• coordina, con il supporto dell'equipe antibullismo, le attività di prevenzione ed informazione sulle sanzioni previste e sulle responsabilità di natura civile e penale, anche con eventuale affiancamento di genitori e studenti;

• si rivolge a partner esterni alla scuola, quali servizi sociali e sanitari, aziende del privato sociale, forze di polizia,.... per realizzare un progetto di prevenzione;

• cura rapporti di rete fra scuole per eventuali convegni/seminari/corsi.

IL COLLEGIO DOCENTI:

• promuove scelte didattiche ed educative, anche in collaborazione con altre scuole in rete, per la prevenzione del fenomeno.

IL TEAM DOCENTI / IL CONSIGLIO DI CLASSE:

• 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 della necessità dei valori di convivenza civile;

• favorisce un clima collaborativo all'interno della classe e nelle relazioni con le famiglie propone progetti di educazione alla legalità e alla cittadinanza attiva.

IL DOCENTE:

• intraprende azioni congruenti con i propri alunni, 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.

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 il proprio figlio, dopo l'uso di internet o del proprio telefonino, mostra stati depressivi, ansiosi o paura);

• conoscono le azioni messe in campo dalla scuola e collaborano secondo le modalità previste dal Patto di corresponsabilità;

• conoscono il codice di comportamento dello studente;

• conoscono le sanzioni previste da regolamento d'istituto nei casi di bullismo, cyberbullismo e navigazione on-line a rischio.

GLI ALUNNI:

• sono coinvolti nella progettazione e nella realizzazione delle iniziative scolastiche, al fine di favorire un miglioramento del clima relazionale;

• possono operare come tutor per altri studenti;

• imparano le regole basilari, per rispettare gli altri, quando sono connessi alla rete, facendo attenzione alle comunicazioni attraverso i social e gli strumenti digitali e non, che inviano;

• non utilizzano durante le lezioni o le attività didattiche in genere cellulari, giochi elettronici e riproduttori di musica, se non per finalità didattiche, previo consenso del docente;

• rispettano il divieto di acquisire durante le attività didattiche o comunque all'interno della scuola, – mediante telefonini cellulari o altri dispositivi elettronici - immagini, filmati o registrazioni vocali, se non per finalità didattiche e previo consenso del docente;

• sono consapevoli che la divulgazione del materiale 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.

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).

Il documento ePolicy ha lo scopo di informare l'intera comunità educante e tutelare i soggetti coinvolti dai rischi connessi all'uso improprio delle tecnologie informatiche e della rete.

A tal proposito le agenzie che erogano attività educative e didattiche, sono tenuti a prendere visione del documento di ePolicy dell'Istituto Comprensivo, incluse le procedure di segnalazione, qualora si verifichino episodi che mettano in pericolo gli studenti.

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

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

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

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

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

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

4 - CONDIVISIONE E COMUNICAZIONE DELLA POLICY ALL'INTERA COMUNITÀ SCOLASTICA

1. Condivisione e comunicazione della Policy agli alunni:

• Saranno dedicate lezioni, adeguate all'età degli alunni, sulle buone pratiche per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta al cyberbullismo.

2. Condivisione e comunicazione della Policy al personale:

• Le norme adottate dalla scuola in materia di sicurezza nell'utilizzo del digitale saranno discusse negli organi collegiali (collegio docenti, consigli di intersezione ed interclasse) e rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito web della scuola;

• Il personale della scuola riceverà un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso materiali resi disponibili anche sul sito web della scuola.

3. Condivisione e comunicazione della Policy ai genitori:

• Le famiglie saranno informate in merito alla linea di condotta adottata dalla scuola per un uso sicuro e responsabile delle tecnologie digitali e di internet attraverso la condivisione del presente documento e di materiali informativi specifici sul sito web della scuola.

• Saranno forniti ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di internet anche a casa: indirizzi sul web relativi a risorse utili per lo studio, siti idonei ed educativi per gli alunni, sistemi di filtraggio, attività educative per il tempo libero.

1.5 - Gestione delle infrazioni alla ePolicy

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

Le infrazioni alla policy possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori a docenti/ATA. Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. Infatti è bene ricordare a tutti che nel momento in

cui un qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia (ex art. 331 del codice di procedura penale). L'omissione di denuncia costituisce reato (art. 361). I reati che, in ambiente scolastico, possono essere riferiti all'ambito digitale e commessi per via telematica sono tra gli altri: -Minaccia; in particolare, se la minaccia è grave, per tale reato si procede d'ufficio (art. 612 cod. pen.); -Induzione alla prostituzione minorile (art. 600bis); -Pedopornografia (art. 600ter); -Corruzione di minorenne (art. 609quinquies).

Per i reati sessuali la magistratura di norma procede su querela di parte; tuttavia nei casi più gravi si persegue d'ufficio e in genere i reati verso le/i minori sono tra quelli per i quali si procede d'ufficio. Nel caso in cui le infrazioni della policy violino norme previste dal Regolamento di Istituto si procede secondo quanto previsto dal Regolamento stesso; qualora le infrazioni riguardino l'opportunità di certi comportamenti o la convivenza civile, la scuola eroga delle sanzioni secondo il principio della sensibilizzazione e del risarcimento dell'eventuale danno provocato, in uno spirito di recupero e rieducazione.

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

· un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;

· l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;

· la condivisione di immagini intime o troppo spinte;

· la comunicazione incauta e senza permesso con sconosciuti;

· il collegamento a siti web non indicati dai docenti. Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo dell'alunno. Infatti più gli alunni sono piccoli, più i comportamenti "da correggere" sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, che devono essere compresi e orientati proprio dagli educatori, nella prospettiva del raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno.

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

· il richiamo verbale;

· il richiamo verbale con particolari conseguenze (riduzione o sospensione

dell'attività gratificante);

· il richiamo scritto con annotazione sul diario;

· la convocazione dei genitori da parte degli insegnanti;

· la convocazione dei genitori da parte del Dirigente scolastico.

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni.

2. Disciplina del personale scolastico Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet sono diverse e alcune possono determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli alunni:

· un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite 'installazione di software o il salvataggio di materiali non idonei;

· un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;

· un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;

· una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;

· una carente istruzione preventiva degli alunni sull'utilizzazione corretta e responsabile delle tecnologie digitali e di internet;

· una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;

· insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale. Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso

a internet, la posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone una copia per eventuali successive investigazioni. Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

3. Disciplina dei genitori In considerazione dell'età degli alunni e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico. Le situazioni familiari meno favorevoli sono:

· la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai;

· una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio;

· una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone;

· un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei;

· un utilizzo del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria indirizzi o contenuti non idonei. I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli,se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

Il presente documento si integra con il Regolamento di Istituto, Il Patto di Corresponsabilità, il Regolamento su Bullismo e Cyberbullismo e il Ptof, incluso il piano dell'attuazione del PNSD.

UTILIZZO DEL LABORATORIO DI INFORMATICA, DELLE POSTAZIONI DI LAVORO E DELL' UTILIZZO DI INTERNET

Disposizioni sull'uso del laboratorio

1. Le apparecchiature presenti nella scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.
2. I laboratori informatici e le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.
3. Quando un insegnante, da solo o in classe, usufruisce del laboratorio deve obbligatoriamente registrare il proprio nome e l'eventuale classe nell'apposito registro delle presenze di laboratorio, indicando l'orario di ingresso, quello di uscita e motivazione dell'uso delle postazioni informatiche. Questo allo scopo di poter risalire alle cause di eventuali inconvenienti o danneggiamenti e per comprovare l'effettivo utilizzo dell'aula.
4. L'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante.
5. Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software.
6. Nei laboratori è vietato utilizzare CD personali o dischetti se non dopo opportuno controllo con sistema di antivirus aggiornato.
7. E' vietato cancellare o alterare files-dati presenti sull'hard disk.
8. Il laboratorio non deve mai essere lasciato aperto o incustodito quando nessuno lo utilizza. All'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il mobilio in ordine, le macchine spente correttamente (chiudi sessione...).
9. In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile del laboratorio.
10. In caso di malfunzionamento non risolvibile dal responsabile di laboratorio si contatterà personalmente o attraverso il Responsabile di laboratorio, la segreteria.
11. Per motivi di manutenzione straordinaria, in caso di guasti o di virus, i PC possono essere formattati senza preavviso. Si consiglia pertanto di salvare i dati importanti su Cd o pen drive periodicamente. In caso di

formattazione ordinaria ci sarà un preavviso.

Disposizioni sull'uso dei software

1. I software installati sono ad esclusivo uso didattico.

2. In base alle leggi che regolano la distribuzione delle licenze, i prodotti software presenti in laboratorio non sono disponibili per il prestito individuale. Nei casi in cui lo fossero in base a precise norme contrattuali i docenti interessati, dopo aver concordato il prestito con il Responsabile di laboratorio, devono compilare l'apposito registro di consegna software custodito in laboratorio.

3. E' fatto divieto di usare software non conforme alle leggi sul copyright. E' cura dell'insegnante utente di verificarne la conformità. Gli insegnanti possono installare nuovo software sui PC del laboratorio della propria scuola, previa autorizzazione scritta del DS solo se il software installato rispetta le leggi sul copyright.

4. E' responsabilità degli insegnanti che chiedono al Responsabile di laboratorio di effettuare copie di cd/dvd per uso didattico, di assicurarsi che la copia non infranga le leggi sul copyright in vigore.

Accesso a internet

1. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante;
2. Internet non può essere usato per scopi vietati dalla legislazione vigente;

3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet;

4. E' vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza.

Norme finali

Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

Si farà, inoltre, riferimento al REGOLAMENTO ANNUALE che il responsabile di

Laboratorio predisporrà per disciplinare l'utilizzo del laboratorio e del materiale in esso presente (notebook, tablet, kit di robotica e digitali)

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il monitoraggio dell'implementazione della Policy avverrà:

- alla fine di ogni anno scolastico, contestualmente al Rapporto di Autovalutazione e sulla base dei casi problematici riscontrati e della loro gestione;

- all'inizio di ogni anno scolastico, contestualmente alla revisione del PTOF, a cura del Dirigente scolastico, dell'Animatore digitale e della commissione E Policy, a seguito di verifica atta a constatare l'insorgenza di nuove necessità e la revisione di tecnologie esistenti

Nell'ambito del monitoraggio dell'implementazione della E-Safety Policy si terranno in considerazione i dati annuali sulla base del seguente documento:

ANNO SCOLASTICO	NUMERO di segnalazioni	NUMERO di infrazioni	NUMERO di sanzioni disciplinari

Il nostro piano d'azioni

Azioni da svolgere entro l'annualità scolastica 2020/21

- Creazione del gruppo di lavoro ePolicy

Azioni da svolgere nei prossimi 3 anni.

- Realizzazione di un sistema di monitoraggio delle attività
- Realizzazione di un'assemblea per discutere delle attività di progetto

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

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

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

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

La scuola sta provvedendo alla costruzione di un curricolo digitale in cui le aree didattiche incontrano i nuclei fondanti dell'educazione alla cittadinanza digitale indicati da DIGICOMP.

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 Piano di Formazione Triennale recepisce le indicazioni contenute nella sezione specifica del Piano Digitale della scuola, prevedendo annualmente corsi di formazione per i docenti sull'utilizzo e integrazione delle TIC nella didattica.

Il Piano Digitale prevede, inoltre, forme di autoformazione in presenza e a distanza relative alla partecipazione ai vari eventi programmati (Codeweek, Hour of Code, Rosa Digitale, ecc).

A seguito dell'emergenza Covid 19, nella scuola è stata effettuata una formazione specifica per tutti i docenti della scuola dell'Infanzia e Primaria sulla piattaforma G Suite for Education e in particolare sull'applicazione Classroom finalizzata all'avvio delle attività di Didattica a Distanza.

2.3 - Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

La scuola ha promosso momenti di formazione informale attraverso l'adesione alle proposte di Generazioni Connesse, come ad esempio al Safer Internet Day.

A partire dall'anno corrente, si è costituito il gruppo E Policy che promuoverà la diffusione della formazione di altri docenti sull'utilizzo consapevole e sicuro di internet e delle tecnologie digitali.

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 scolastico provvede a sensibilizzare ed informare le famiglie sulle tematiche relative all'uso consapevole e responsabile delle tecnologie digitali attraverso l'aggiornamento dei regolamenti, del Patto di Corresponsabilità e della sezione dedicata sul sito web istituzionale.

Il nostro piano d'azioni

Piano di azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021)

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

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

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.

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

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

personali.

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 ai fini della protezione e sicurezza degli stessi. All'inizio dell'anno scolastico, i genitori sottoscrivono un'informativa sul trattamento dei dati personali in ottemperanza all'art. 13 D.Lgs 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali). I genitori rilasciano, inoltre, il consenso all'utilizzo di materiale fotografico e audiovisivo riservato e di elaborati degli alunni per esporli anche in sedi diverse da quelle dell'Istituto quali pubblicazioni in formato digitale e sito web della scuola.

In caso di utilizzo di piattaforme digitali condivise o di strumenti per la creazione e la gestione di classi virtuali viene acquisito preventivamente il consenso informato dei genitori. In caso di attività di ampliamento dell'offerta formativa, organizzate in collaborazione con Enti esterni, viene richiesto ai genitori un ulteriore consenso informato alle riprese audio/video e al loro eventuale utilizzo per scopi didattici, informativi e divulgativi anche tramite pubblicazione su siti web.

a) Pratiche strategiche e operative

La responsabilità del trattamento dei dati personali è esercitata dal dirigente scolastico.

● Il Dirigente Scolastico è il responsabile della gestione dei rischi relativi a questo ambito.

● Il Dirigente scolastico designa quali incaricati al trattamento dei dati, il DSga e il personale amministrativo.

● il DSga, cui è conferito dal Dirigente il compito di sovrintendere/amministrare il sistema di gestione e custodia dei dati personali, individua gli incaricati del trattamento dei dati medesimi.

● Il personale amministrativo è istruito sulla procedura da seguire per segnalare eventuali incidenti dove la protezione dei dati potrebbe essere stata compromessa.

b) Soluzioni tecniche

Il personale ha un'area protetta sulla rete per memorizzare i file sensibili (segreteria digitale e registro elettronico)

● Tutti i server sono in posizioni bloccabili e gestiti da personale interno

● la segreteria adotta:

- password;

- individua soggetti preposti alla gestione delle password;

- ha un codice identificativo personale per ogni utente;

- ha programmi antivirus;

- protegge e regolamenta gli accessi ai locali che ospitano i dati riservati o in cui si trovano le postazioni di lavoro che ne consentono l'accesso;

- definisce i criteri per garantire l'integrità dei dati;

- definisce i criteri per garantire la trasmissione sicura dei dati.

Si dota di mezzi elettronici adeguati per impedire l'accesso dall'esterno alla rete della segreteria, quali Firewall o simili.

L'accesso ai dati riportati nel registro elettronico (valutazioni) è riservato ai genitori tramite la consegna di una password strettamente personale.

3.2 - Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti

e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola".

Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

L'accesso a internet è possibile in tutte le aule di ogni sede dell'Istituto Comprensivo e nei laboratori d'informatica. Le impostazioni sono definite e manutenute dal responsabile esterno ed è in carico a ciascun docente la segnalazione di malfunzionamenti e disservizi. I docenti hanno piena autonomia nel collegamento ai siti web nelle postazioni a loro riservate. Relativamente agli alunni che accedono a Internet durante l'attività didattica sono consentiti la navigazione guidata da parte dell'insegnante e la stesura di documenti collaborativi purché sotto il controllo dell'insegnante e nel caso in cui tale attività faccia parte di un progetto di lavoro precedentemente autorizzato.

Per l'avvio delle attività di didattica a distanza, l'Animatore Digitale ha predisposto l'accesso alla piattaforma G Suite for Education e all'applicazione Classroom fornendo le credenziali a tutto il personale e a tutte le famiglie della scuola dell'Infanzia, Primaria e Secondaria di Primo grado.

Ogni docente e ogni famiglia accede al registro elettronico attraverso una password personale che non può essere comunicata a terzi, né agli alunni.

3.3 - Strumenti di comunicazione online

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

Il sito dell'Istituto Scolastico è http://www.comprensivonardo2.edu.it/

Il sito prevede un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali, avvisi di carattere generale, e un'area riservata accessibile solo dopo autenticazione.

Il personale che è in possesso delle credenziali per la gestione dei contenuti sul portale si assumerà la responsabilità editoriale di garantire che il contenuto inserito sia accurato e appropriato.

Il Dirigente e il Responsabile del Sito verificano i contenuti destinati alla pubblicazione.
L'Animatore digitale ha associato al dominio coprensivonardo2.edu.it la piattaforma G Suite for Education, di cui ne gestisce le impostazioni e gli account per tutti gli studenti, i docenti e il personale in servizio nell'Istituto.

3.4 - Strumentazione personale

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

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

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

- docenti

Durante le ore delle lezioni è consentito l'utilizzo di qualsiasi dispositivo elettronico personale SOLO a scopo didattico ad integrazione di quelli scolastici. Durante il restante orario di servizio è consentito l'utilizzo del cellulare esclusivamente per comunicazioni personali di carattere urgente.

- personale della scuola

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

Il nostro piano d'azioni

Piano di azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021):

- Organizzare uno o più eventi o attività volti a consultare i docenti e rappresentanti dei genitori in seno al Consiglio di Circolo dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli alunni della scuola sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli alunni della scuola sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali

personali.

- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli alunni della scuola sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto Scolastico sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli alunni della scuola 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.*

Come scuola intendiamo per prevenzione un insieme molto ampio di strategie che coinvolgano le famiglie e le forze sociali che operano sul territorio al fine di mettere al proprio centro l'educazione formativa dei ragazzi.
La Scuola ha scelto una politica interna che sia pro-attiva, tesa cioè a creare un ambiente di apprendimento sereno e sicuro in cui sia chiaro sin dal primo giorno di scuola che (cyber)bullismo, prepotenza, aggressione e violenza non sono permessi, in cui ci sia l'apertura necessaria all'incoraggiamento a parlare di sé e dei propri problemi, che stimoli alla partecipazione diffusa di

tutta la comunità scolastica e che insegni ad interagire in maniera responsabile.

Nello specifico, la scuola attiverà una serie di misure:
- integrare nel curricolo temi legati al corretto utilizzo delle TIC e di Internet;
- progettare unità didattiche specifiche che verranno pianificate a livello di interclasse, garantendo un intervento su ogni classe, anche con docenti non titolari della classe;
- supportare e implementare la competenza digitale in tutti i ragazzi all'interno delle materie curricolari.

La scuola si avvale, inoltre, della collaborazione di enti e associazioni per realizzare incontri rivolti agli alunni e alle famiglie con l'intento di fornire ogni elemento utile alla prevenzione e alla gestione dei problemi relativi alla sicurezza informatica.

La nostra scuola attiva inoltre un "punto di ascolto" al quale gli alunni si possono rivolgere per comunicare attraverso messaggi la propria richiesta di aiuto.

RISCHI	AZIONI
Adescamento online (grooming)	Sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione. Qualora si venga a conoscenza di casi simili, occorre valutarne la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.
Cyberbullismo	Campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni. I casi possono essere molto variegati, variando dal semplice scherzo di cattivo gusto via sms/Whatsapp a vere e proprie minacce verbali e fisiche, che costituiscono reato. Occorre confrontarsi con il Dirigente Scolastico sulle azioni da intraprendere.
Dipendenza da Internet, videogiochi, shopping o gambling online, ...	Informazioni sul fatto che ciò può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito a insaputa di altri) rappresenta un vero e proprio illecito.

Esposizione a contenuti pornografici, violenti, razzisti, ...	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione e sensibilizzazione sulla necessità di monitorare l'esperienza online dei propri figli. Verso gli alunni: inserimento nel curricolo di temi legati alla affidabilità delle fonti online, all'interculturalità e al rispetto delle diversità. Qualora si venga a conoscenza di casi simili, occorre convocare i genitori per richiamarli a un maggiore controllo sulla fruizione di Internet da parte dei propri figli e/o sulla necessità di non usufruirne in presenza degli stessi.
Sexting e pedopornografia.	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione. Verso gli alunni: inserimento nel curricolo di temi legati all'affettività, alla sessualità e alle differenze di genere. In casi simili, se l'entità è lieve occorre in primo luogo parlarne con alunne e alunni e rispettivi genitori, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. Chi è immerso dalla nascita nelle nuove tecnologie spesso non è consapevole che una foto o un video diffusi in rete potrebbero non essere tolti mai più né è consapevole di scambiare o diffondere materiale pedopornografico. In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico per gli adempimenti del caso.
Violazione della privacy	Informazione sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farle rispettare. Se il comportamento rilevato viola solo le norme di buona convivenza civile e di opportunità, occorre convocare i soggetti interessati per informarli e discutere dell'accaduto e concordare forme costruttive ed educative di riparazione. Qualora il comportamento rappresenti un vero e proprio illecito, il Dirigente Scolastico deve esserne informato in quanto a seconda dell'illecito sono previste sanzioni amministrative o penali.

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**. Per segnalazioni di pedopornografia: www.generazioniconnesse.it, sezione **"Segnala contenuti illegali"** (Hotline).

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).

Uno dei più importanti studiosi di bullismo, Peter Smith, definisce il cyberbullismo "una forma di prevaricazione volontaria e ripetuta, attuata attraverso un testo elettronico, a danno di un singolo o un gruppo con l'obiettivo di ferire e mettere a disagio la vittima di tale comportamento che non riesce a difendersi". Il cyberbullismo o bullismo elettronico comprende quindi tutte le forme di prevaricazione e prepotenze tra coetanei messe in atto attraverso e-mail, messaggini con i cellulari, chat, blog, siti internet, immagini o video diffusi sulla rete. L'obiettivo del bullo è sempre lo stesso: molestare la vittima, minacciarla, deriderla.

Gli alunni di oggi, "nativi digitali", hanno ottime competenze tecniche ma allo stesso tempo mancano ancora di pensiero riflessivo e critico sull'uso delle tecnologie digitali e di consapevolezza sui rischi del mondo digitale. Il confine tra uso improprio e uso intenzionalmente malevolo della tecnologia, tra incompetenza e premeditazione, è sottile. In questo quadro, lo spazio online può diventare un luogo dove il bullismo inizia o è mantenuto.

Il 18 giugno 2017 è entrata in vigore la Legge n.71/2017 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo", ossia il primo strumento legislativo per contrastare il

sempre più dilagante fenomeno del cyberbullismo, attraverso un approccio più "educativo" che "repressivo".

Ai fini di tale legge, 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".

A differenza del bullo tradizionale, nel cyberbullo - che già agisce nell'anonimato - viene a mancare un feedback diretto sugli effetti delle aggressioni perpetrate a causa della mancanza di contatto diretto con la vittima. La tecnologia consente ai bulli, inoltre, di infiltrarsi nelle case e nella vita delle vittime, di materializzarsi in ogni momento, perseguitandole con messaggi, immagini, video offensivi inviati tramite diversi device, o pubblicati su siti web tramite Internet.

Ci sono alcune particolari caratteristiche che differenziano il cyberbullismo dal bullismo tradizionale:

• **anonimato**: spesso il bullo si nasconde dietro nomi falsi, un nickname, pensando di non poter essere scoperto;

• **assenza di relazione tra vittima e bullo**: per chi subisce le molestie è ancora più difficile difendersi, perché molto spesso le vittime non riescono neppure a individuare chi è il bullo;

• **mancanza di feedback emotivo**: il cyberbullo, non vedendo le reazioni della vittima ai suoi comportamenti, non è mai totalmente consapevole del danno che arreca, questo lo rende più disinibito e abbassa i livelli di autocontrollo;

• **spettatori infiniti:** le persone che possono assistere ad episodi di cyberbullismo sono potenzialmente illimitate. La diffusione in rete è incontrollabile e non avviene con un gruppo di persone definito.

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.

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?

Da implementare con le indicazioni contenute nella lezione.

4.5 - Sexting

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

impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

Da implementare con le indicazioni contenute nella lezione.

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.

Da implementare con le indicazioni contenute nella lezione.

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.

Da implementare con le indicazioni contenute nella lezione.

Il nostro piano d'azioni

Piano di azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021):

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

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

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

. Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli alunni, con il coinvolgimento di esperti.

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

- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli alunni.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

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

Si considerano da segnalare tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o un piccolo gruppo) tramite un utilizzo irresponsabile dei social network.

In particolare, si segnaleranno:

- contenuti afferenti alla violazione della privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);

- contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);

- contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

Tutte le segnalazioni riportate dai docenti verranno registrate su apposita scheda.

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.

Nella fase di primo intervento possono risultare utili ai docenti i seguenti documenti che vengono allegati:

- VADEMECUM
- MODULO PER LA SEGNALAZIONE
- MODULO PER IL FOLLOW-UP DEI CASI.

VADEMECUM

In questa scheda puoi trovare alcuni indicatori (sotto forma di domande-stimolo e/o consigli) per verificare se nella tua classe ci possono essere episodi di cyberbullismo/bullismo.
Ricorda che è più facile accorgersi di episodi di bullismo, che possono avvenire anche sotto il tuo sguardo, piuttosto che di cyberbullismo, dove le prevaricazioni vengono perpetrate nei luoghi virtuali in cui bambini e adolescenti si ritrovano (in particolare i social).

Ricorda che l'elenco non è esaustivo di ciò che puoi osservare (la realtà è sempre più complessa di come la si può descrivere); gli indicatori sono segnali ai quali dovresti prestare attenzione ma che non hanno la pretesa di identificare in modo assoluto una situazione di cyberbullismo, soprattutto se considerati isolatamente.

Se hai il dubbio che un tuo alunno/a possa essere preso di mira da cyberbulli, ti invitiamo a riflettere sulle seguenti domande/stimolo.

- Hai alunni che mostrano segnali di tensione o nervosismo quando ricevono messaggi durante le attività didattiche strutturare e preventivamente stabilite?

- Hai alunni che si mostrano timorosi o preoccupati durante attività che richiedono connessione?

- Hai alunni che presentano comportamenti / abitudini che causano irritazione in compagni e adulti (che, ad esempio, vengono isolati online dai compagni)?

- Hai alunni che non sono inseriti o sono stati esclusi dai gruppi dei servizi di messaggistica istantanea (Whatsapp, telegram, viber, etc.) o social della classe?
Se hai il dubbio che un tuo alunno/a possa essere preso di mira da bulli, ti invitiamo a riflettere sulle seguenti domande/stimolo.
- Hai alunni che passano molto tempo da soli (per esempio durante gli intervalli o le ore di Educazione Fisica), che vengono sistematicamente esclusi dal gruppo-classe (non hanno amici nel gruppo classe, vengono scelti per ultimi nei lavori di gruppo) o che ricercano la vicinanza degli adulti anche nei momenti di intervallo preferendo parlare con un insegnante o un operatore scolastico o stare soli piuttosto che nel gruppo dei pari?

- Hai alunni che sono diventati più insicuri e spaventati quando parlano in classe davanti ai compagni?

-Hai notato o sai che questo stesso comportamento non l'hanno in altri contesti o quando devono parlare a degli adulti? Non era mai accaduto prima?

-Hai alunni che hai sempre reputato bravi e che invece da qualche tempo a questa parte hanno avuto un calo nel rendimento scolastico per il quale non riesci a comprenderne le cause? o che subiscono ripetutamente il furto, il danneggiamento e la dispersione di oggetti o beni materiali (libri, merenda, denaro)?

- Hai alunni che nell'ultimo periodo mostrano cambiamenti nei comportamenti, in particolare si sono chiusi in se stessi, parlano meno con i compagni di classe e sembrano in costante stato di allerta e paura? o che reagiscono in modo impulsivo o aggressivo a quelle che a tuo avviso sono battute o scherzi tra compagni?

- Hai alunni che nell'ultimo periodo hanno fatto assenze frequenti senza che i colloqui con i genitori ti abbiano aiutato a scoprirne le cause?

Ricorda che, nei casi più estremi il bambino preso di mira dai compagni potrebbe arrivare a provocarsi ferite volontariamente o minacciare fughe o esplicitare il desiderio di togliersi la vita: tutti questi segnali denotano un

malessere che, anche se non esplicitato in modo diretto, è sintomo di una causa da ricercare.

Se pensi che qualche alunno/a possa essere bullo o cyberbullo, ti invitiamo a riflettere sulle seguenti domande/stimolo:
- Hai alunni con la tendenza a prendere in giro sempre le stesse persone, anche attraverso post online o foto o messaggi vocali di cui altri alunni si lamentano?

- Hai alunni che mostrano una tendenza costante ad avere comportamenti prevaricatori o di comando nei riguardi dei compagni? o che nei social o nel gruppo whatsapp della classe "governano" le conversazioni?

- Hai alunni che faticano ad essere empatici nei confronti di qualche compagno che ha subito il furto di un oggetto in classe? O che mostrano disattenzione rispetto agli stati emotivi di chi è in difficoltà? O che fatica a smettere di prendere in giro un compagno a motivo di qualcosa visto sul suo profilo online?

Se riconosci nelle situazioni descritte, anche solo in parte, ciò che accade nella tua classe, può esserti utile approfondire la situazione sia coinvolgendo la classe che la comunità scolastica o confrontandoti con esperti chiedendo supporto alla Helpline di Generazioni Connesse al numero 1.96.96 per capire come approfondire la situazione e offrire ai minori coinvolti, se lo desiderano, l'eventuale supporto necessario.
Il cyberbullismo è un fenomeno relazionale e per contrastarlo ed affrontarlo occorre l'impegno di tutti.

Nome di chi segnala	
Ruolo	
Data	
Descrizione dell'episodio o del problema	
Soggetti coinvolti	Vittima/e Classe Bullo/i Classe
Chi ha riferito dell'episodio?	☐La vittima ☐Un compagno della vittima, nome: ☐ Genitore, nome: ☐Insegnante, nome: ☐Altri, specificare:
Atteggiamento del gruppo	Da quanti compagni è sostenuto il bullo? Quanti compagni supportano la vittima o potrebbero farlo?
Gli insegnanti sono intervenuti in qualche modo?	
La famiglia o altri adulti hanno cercato di intervenire?	
Chi è stato informato della situazione?	☐ coordinatore di classe data ☐ consiglio di classe data ☐ dirigente scolastico data ☐ la famiglia della vittima/e data ☐ la famiglia del bullo/i data ☐ le forze dell'ordine ☐ altro (specificare:____)

MODULO FOLLOW UP

AZIONI INTRAPRESE	La situazione è:

Aggiornamento 1 Data:	☐ migliorata ☐ invariata ☐ peggiorata In che modo?
Aggiornamento 2 Data:	☐ migliorata ☐ invariata ☐ peggiorata In che modo?
Aggiornamento 3 Data:	☐ migliorata ☐ invariata ☐ peggiorata In che modo?

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.

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.

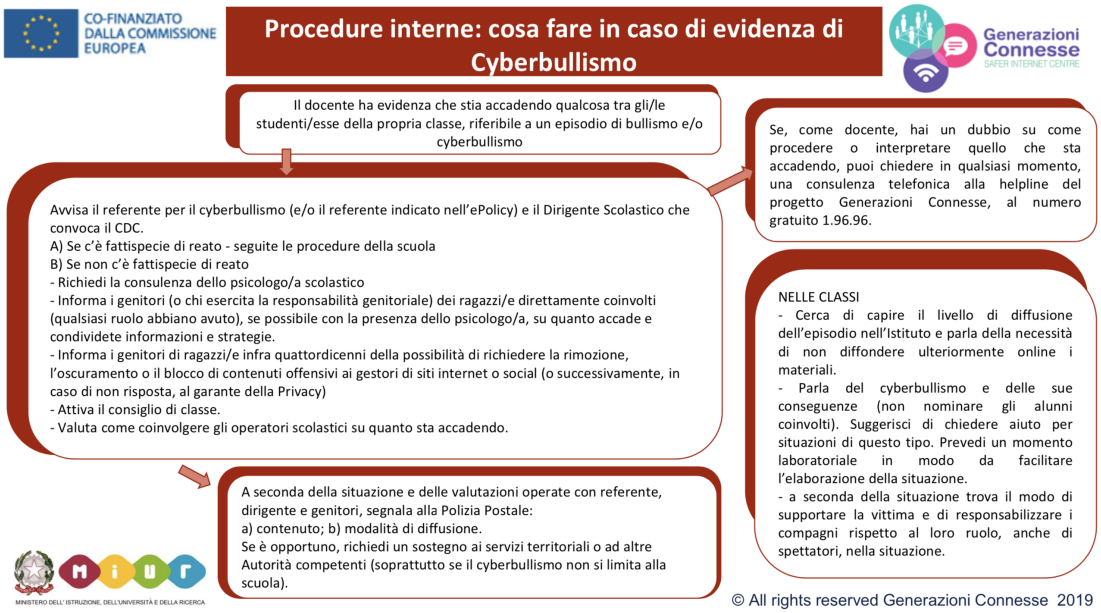
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare 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

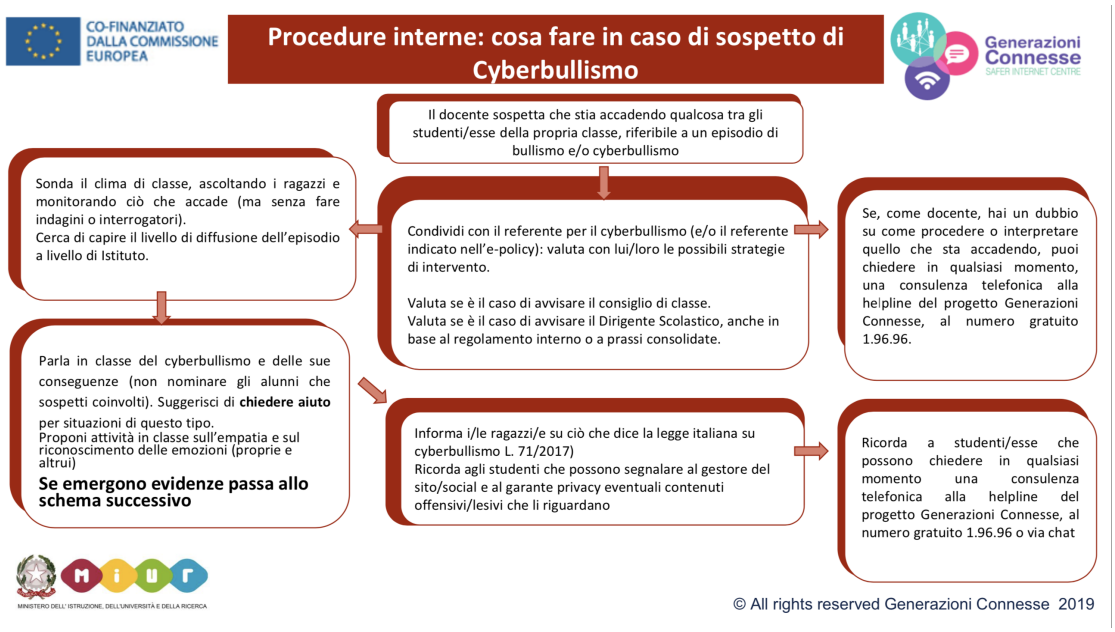
alle situazioni di rischio correlate.

- **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 in quanto vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

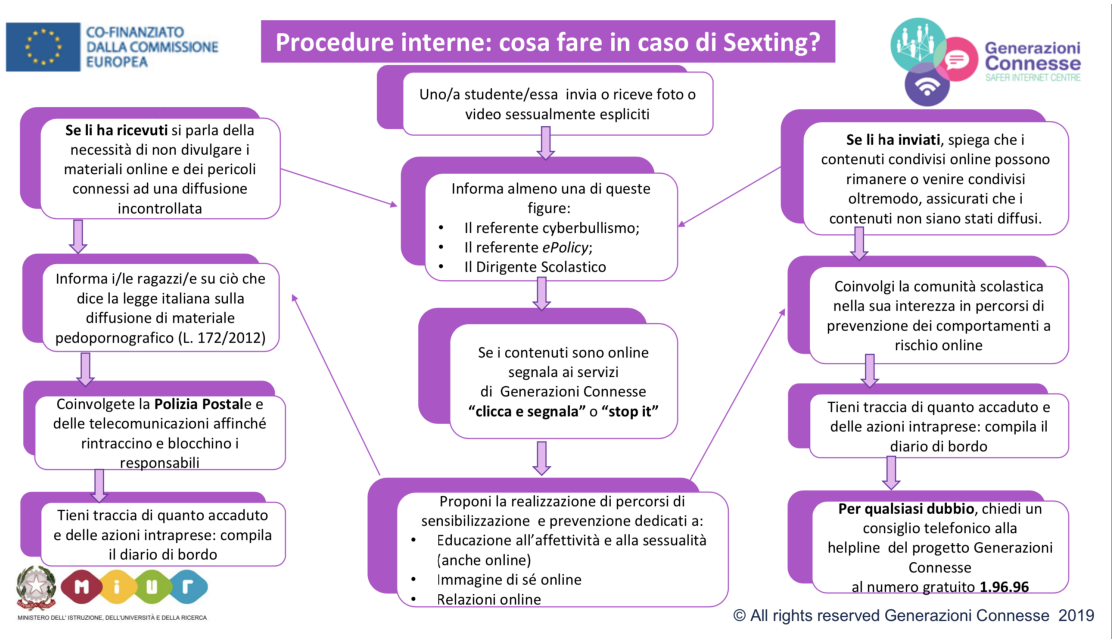
5.4. - Allegati con le procedure

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

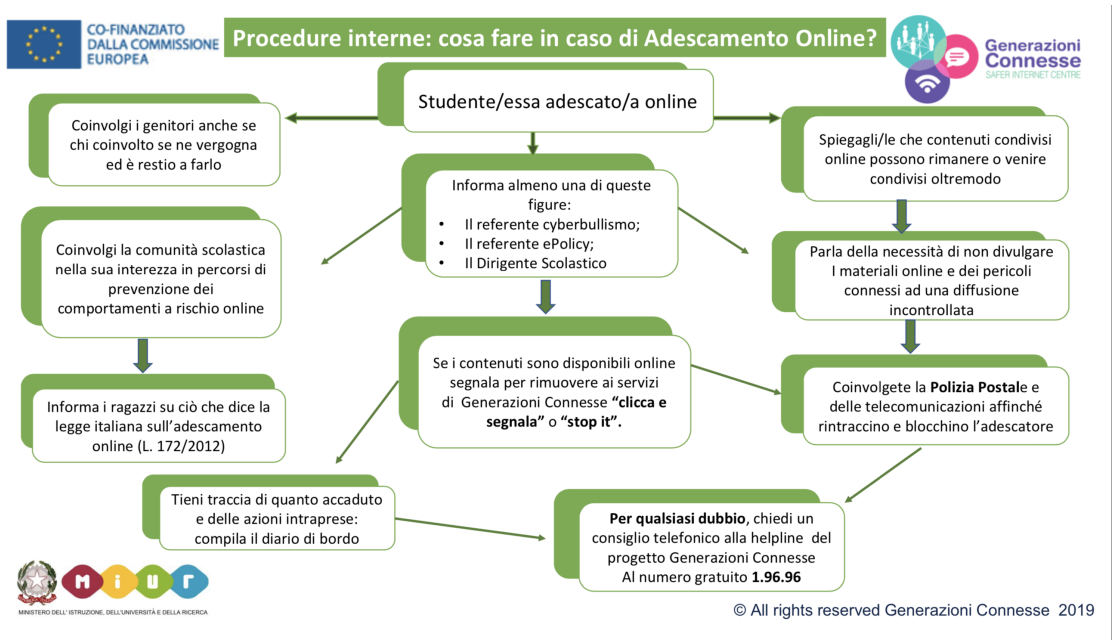




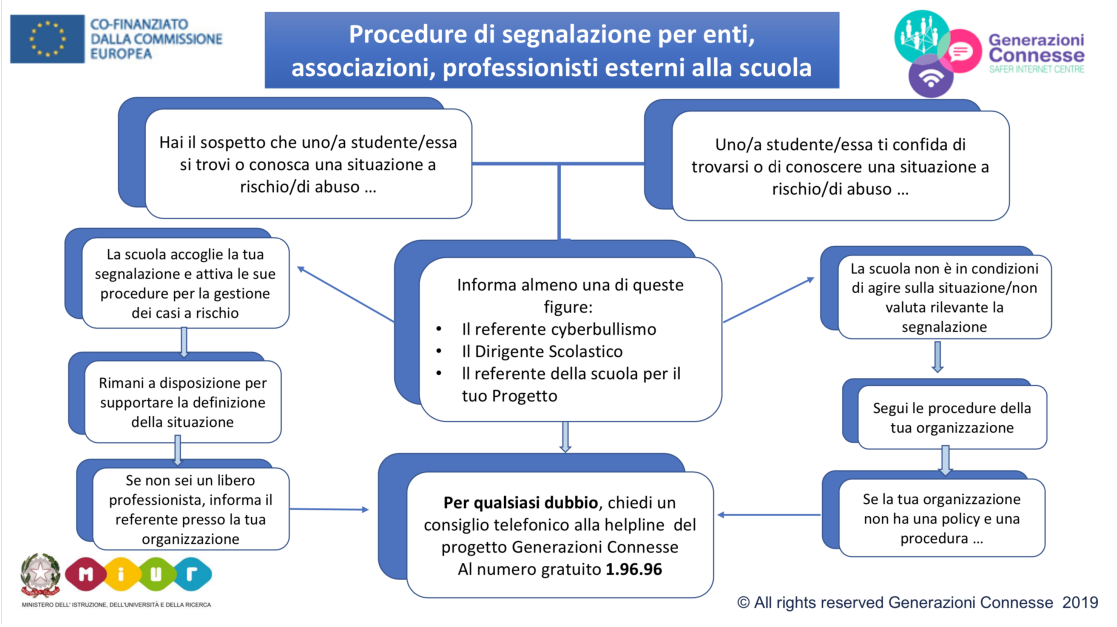
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

- Scheda di segnalazione

- Diario di bordo
- iGloss@ 1.0 l'ABC dei comportamenti devianti online
- Elenco reati procedibili d'ufficio

Il nostro piano d'azioni

Non è prevista nessuna azione.