LICEO SCIENTIFICO STATALE - "GIANCARLO SIANI"-AVERSA
Prot. 0002787 del 30/11/2020
(Uscita)

Documento di ePolicy

CEPS14000X

GIANCARLO SIANI

VIALE EUROPA 269 - 81031 - AVERSA - CASERTA (CE)

ROSARIA BARONE

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.

Perché è importante dotarsi di una E-policy?

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la

comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.

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

Il documento vuole presentare in maniera esaustiva e chiara le linee guida del Liceo Scientifico Statale "G.Siani" in materia di:

- utilizzo consapevole delle TIC negli ambienti scolastici e nella didattica;
- prevenzione/gestione di situazione problematiche relative all'uso delle tecnologie digitali;
- segnalazione dei casi individuati all'interno della scuola;
- gestione dei casi, ovvero le misure che la scuola intende attivare a supporto delle famiglie e degli studenti vittime o spettatori attivi e/o passivi di quanto avvenuto.

Il nostro Istituto sta aderendo al progetto GENERAZIONI CONNESSE, promosso dal MIUR in collaborazione con l'Unione Europea.

Ha elaborato il presente documento in conformità con le LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrasto del bullismo e del cyberbullismo emanate dal Ministero dell'Istruzione, dell'Università, della Ricerca in collaborazione con il Safer Internet Center per l'Italia.

Si premette:

a) il progetto "Generazioni connesse" sarà inserito nel nostro Piano Triennale dell'Offerta Formativa;

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.

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.

Dirigente Scolastico

Nel promuovere l'uso consentito delle tecnologie e di internet, il ruolo del Dirigente Scolastico è quello di:

- garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i

membri della comunità scolastica;
- garantire ai propri docenti una formazione di base sulle Tecnologie dell'Informazione e della Comunicazione (ICT) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse;
- garantire l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza online;
- dover informare tempestivamente, qualora venga a conoscenza di atti di cyberbullismo, che non si configurino come reato, i genitori dei minori coinvolti (o chi ne esercita la responsabilità genitoriale o i tutori);
- regolare il comportamento degli studenti ed imporre sanzioni disciplinari in caso di comportamento inadeguato, in relazione all'utilizzo delle TIC.

Referente Cyberbullismo d'Istituto

Il ruolo del Referente per Bullismo e Cyberbullismo include i seguenti compiti:

- coordina iniziative di prevenzione e contrasto del cyberbullismo messe in atto dalla scuola, anche avvalendosi della collaborazione delle Forze di Polizia, nonché delle associazioni e dei centri di aggregazione giovanile presenti sul territorio;
- svolge un importante compito di supporto al Dirigente, nonché all'Istituzione scolastica, per la revisione/stesura di Regolamenti, atti e documenti (PTOF, PdM, RAV, modello di e-policy d'Istituto);
- promuove la conoscenza e la consapevolezza riguardo a bullismo e cyberbullismo, attraverso progetti d'Istituto che coinvolgano genitori, studenti e personale scolastico;
- collabora in team con altre figure scolastiche (Animatore Digitale; Referente BES/Inclusione; Referente per la Dispersione);
- segnala tempestivamente situazioni di rischio online o casi di bullismo o cyberbullismo;
- suggerisce, incentiva e supporta progetti di Istituto relativi allo sviluppo nei discenti delle Competenze di Cittadinanza e Costituzione, nonché progetti di prevenzione ed informazione/formazione dell'intera comunità scolastica;
- coinvolge gli altri soggetti della comunità scolastica, con particolare attenzione agli studenti/ex studenti (PEER EDUCATION);
- può attivare uno SPORTELLO anonimo di segnalazione.

Animatore Digitale e Team dell'Innovazione

Il ruolo dell'Animatore Digitale, coadiuvato dal Team per l'Innovazione, include i seguenti compiti:

- stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza ed informazioni al personale in relazione ai rischi online ed alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle TIC e di internet a scuola, nonché approntarsi all'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite passwords applicate e regolarmente cambiate;

- coinvolgere l'intera comunità scolastica (alunni, genitori ed altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".

Tecnico informatico

Il ruolo del tecnico informatico si compone dei seguenti compiti:

- può controllare ed accedere a tutti i files della intranet;
- installa nuovi software;
- limita attraverso un proxy l'accesso ad alcuni siti;
- controlla e coordina, con l'ausilio di un opportuno registro, la prenotazione dei laboratori, consentendo in tal modo di tenere traccia di orari, laboratori e supporti utilizzati da ciascuno.

Direttore dei Servizi Generali e Amministrativi

Il ruolo del DSGA include i seguenti compiti:

- assicurare, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione necessari ad evitate un cattivo funzionamento della dotazione tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate.

Docenti

Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti:

- provvedere personalmente alla propria formazione/aggiornamento sull'utilizzo del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in Internet e dell'immagine degli altri: lotta al cyberbullismo);
- supportare gli alunni nell'utilizzo consapevole delle tecnologie informatiche utilizzate a scopi didattici ed informarli/formarli sul divieto di plagio e sul rispetto della normativa vigente in merito ai diritti d'autore;
- segnalare al Dirigente scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazioni;
- supportare ed indirizzare alunni coinvolti in problematiche legate alla rete.

Personale ATA

Il personale è tenuto ad assicurarsi di:

- avere adeguata consapevolezza riguardo alle questioni di sicurezza informatica, alla politica d'Istituto e relative buone pratiche;
- aver letto, compreso ed accettato il presente documento di E-Safety Policy;
- segnalare qualsiasi abuso, anche solo sospetto, al Dirigente Scolastico e/o all'Animatore Digitale per le opportune indagini/azioni/sanzioni;
- mantenere tutte le comunicazioni digitali con alunni e genitori/tutori a livello professionale e realizzandole esclusivamente attraverso canali ufficiali scolastici.

Studenti

Il ruolo degli studenti prevede i seguenti compiti:

- leggere, comprendere ed accettare il documento di E-Safety Policy;
- comprendere e rispettare le norme sul diritto d'autore;
- avere consapevolezza delle situazioni di rischio legate alla rete, telefoni cellulari, fotocamere digitali;
- conoscere la politica della scuola sull'uso di dispositivi mobili e sull'uso delle immagini;
- comprendere l'importanza di adottare buone pratiche di sicurezza online quando si usano le tecnologie;
- adottare condotte rispettose degli altri anche durante la comunicazione in rete; comprendere l'importanza della segnalazione di ogni abuso, uso improprio, o accesso a materiali inappropriati, e conoscere il protocollo per tali segnalazioni;
- essere consapevoli del significato e della gravità di atti di cyberbullismo, a tutela della propria ed altrui incolumità, al fine di evitare di perpetrare violazioni al Regolamento d'Istituto ed al Patto di Corresponsabilità o, nei casi più gravi, reati punibili da parte della Magistratura;
- assumersi la responsabilità di un eventuale utilizzo sbagliato delle tecnologie.

Genitori

Genitori e tutori svolgono un ruolo cruciale nel garantire che i minori comprendano la necessità di utilizzare in modo sicuro, consapevole ed appropriato dispositivi digitali e mobili. Per tale scopo è necessario che essi:

- contribuiscano, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- incoraggino l'impiego delle ICT da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza;
- sostengano l'Istituzione scolastica nel promuovere le buone pratiche di e-safety e, dunque, seguano le linee guida sull'uso appropriato di immagini digitali e video registrati in occasione di eventi scolastici, anche al di fuori delle aule;
- consultino periodicamente le sezioni del sito web loro dedicate, con particolare riguardo ed attenzione alla consultazione del registro elettronico;
- agiscano in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite;
- rispondano per gli episodi commessi dai figli minori a titolo di culpa in educando (articolo 2048 del Codice civile). Infatti, sono esonerati da responsabilità solo se dimostrano di non aver potuto impedire il fatto. Ma nei casi più gravi per i giudici l'inadeguatezza dell'educazione impartita ai figli emerge dagli stessi episodi di bullismo, che per le loro modalità esecutive dimostrano maturità ed educazione carenti.

Enti educativi esterni ed associazioni

Gli enti educativi esterni e le associazioni, che entrano in relazione con l'istituzione scolastica, hanno il compito di:

- osservare le politiche interne sull'uso consapevole della Rete e delle TIC.
- attivare procedure e comportamenti sicuri per la protezione degli studenti e delle studentesse, durante le attività che vengono svolte all'interno della scuola o in cui sono impegnati gli stessi.

Per quanto non espressamente indicato sui ruoli e sulle responsabilità delle figure presenti all'interno dell'Istituzione scolastica, si rimanda: all'art. 21, comma 8, Legge 15 marzo 1997, n. 59; all'art. 25 della Legge 30 marzo 2001, n. 165; al CCNL in vigore; al D.P.R. 8 marzo 1999, n. 275; alla Legge 13 luglio 2015, n. 107; al Piano Nazionale Scuola Digitale; a quanto statuito in materia di culpa in vigilando, culpa in organizzando, culpa in educando.

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

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

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

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

.

1.4 - Condivisione e comunicazione

dell'ePolicy all'intera comunità scolastica

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

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

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

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

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

Il Documento E-Policy è stato redatto dal gruppo di lavoro composto dai docenti Rosa Tamburrino Cerullo (referente), Stefania Febbraro, Sonia Ebraico e Annunziata Pagano.

I docenti componenti il gruppo di lavoro hanno seguito una formazione online apposita ai fini della redazione di tale documento.

Onde evitare che l'adozione del presente documento rappresenti un mero atto formale, l'Istituto si impegna ad intraprendere una serie di azioni ed iniziative per la messa in atto della Policy. Oltre alla condivisione con l'intera comunità scolastica attraverso la pubblicazione sul sito della scuola, si possono prevedere, ad esempio:

per il corpo docente:

- discussione in ambito collegiale sui contenuti, sulle pratiche indicate e su come declinare nel curriculo le tematiche d'interesse della policy;
- confronto collegiale, a cadenza annuale, riguardo alla necessità di apportare eventuali modifiche e/o miglioramenti alla policy vigente;
- elaborazione di protocolli condivisi di intervento;

per la componente studentesca:

- discussione in classe con il coordinatore sulla policy, nei primi giorni di attività scolastica, con particolare riguardo al protocollo di accoglienza per le nuove classi prime;
- diffusione tra gli studenti di un estratto del documento relativo, in particolare, ai comportamenti da attuare in caso di bisogno;
- lettura, comprensione e sottoscrizione del patto di corresponsabilità;

per i genitori:

- organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o stigmatizzare;
- lettura e comprensione del Regolamento d'Istituto e sottoscrizione del Patto di Corresponsabilità.

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.

Infrazioni degli alunni

È bene che i docenti introducano, preventivamente, attività laboratoriali miranti a sviluppare nei loro alunni una sempre maggiore consapevolezza dei rischi legati a un uso imprudente e improprio del web e che forniscano loro, ogni qualvolta avvenga un'infrazione alle regole stabilite, gli strumenti per affrontare le conseguenze dei loro errori. Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola utilizzando le TIC ed internet, messi a loro disposizione a fini puramente didattici, sono prevedibilmente le seguenti:

- uso improprio della rete per esprimere giudizi, infastidire o impedire a qualcuno di esprimersi liberamente o partecipare al dialogo didattico-educativo;
- l'invio incauto o non autorizzato di immagini, foto o dati sensibili; la condivisione di immagini non appropriate, violente, intime o troppo spinte;
- la comunicazione incauta e non autorizzata con sconosciuti o soggetti comunque estranei all'azione didattico-educativa;
- il collegamento a siti web non indicati e, dunque, non autorizzati dai docenti durante attività laboratoriali di qualsiasi genere.

I provvedimenti disciplinari da adottare da parte dei consigli di classe nei confronti di alunni che abbiano commesso una o più infrazione alla policy, secondo quanto sopra, (in proporzione sia all'età dello studente sia alla gravità dell'infrazione commessa) saranno i seguenti:

- richiamo verbale;
- sanzioni estemporanee commisurate alla gravità della violazione commessa;
- nota informativa ai genitori o tutori mediante registro elettronico;
- convocazione dei genitori o tutori per un colloquio con gli insegnanti;
- convocazione dei genitori o tutori per un colloquio con il Dirigente scolastico.

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi di eventuali disagi causati; di ridefinizione delle regole sociali di convivenza, attraverso la partecipazione consapevole ed attiva degli alunni delle classi coinvolte; di prevenzione

e gestione positiva dei conflitti; di moderazione dell'eccessiva competitività, promozione dei rapporti amicali e di reti di solidarietà, di promozione della conoscenza e gestione delle emozioni.

Infrazione del Personale Scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico ed in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet sono quelle potenzialmente atte a determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli studenti:

- utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli studenti, estraneo all'attività di insegnamento od al proprio profilo professionale, anche tramite l'installazione di software od il salvataggio di materiali non idonei;
- utilizzo delle comunicazioni elettroniche con genitori e/o alunni non compatibile con il proprio ruolo professionale;
- trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- diffusione delle password assegnate e custodia incauta degli strumenti e degli accessi, di cui potrebbero approfittare terzi;
- carente istruzione preventiva degli studenti sul corretto e responsabile utilizzo delle TIC e di internet;
- mancata o non attenta vigilanza degli studenti, che potrebbe favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- insufficiente azione di contrasto a terzi in situazioni critiche; di interventi correttivi o di sostegno a studenti;
- mancata segnalazione al Dirigente, all'Animatore Digitale, ai genitori, in situazioni critiche.

Il Dirigente Scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle norme di sicurezza, compreso l'accesso ad internet e la posta elettronica inviata/pervenuta a scuola; procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone copia per eventuali successive investigazioni. Tutto il personale è tenuto a collaborare con il Dirigente Scolastico ed a fornire ogni informazione utile alle valutazioni del caso ed all'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. Le infrazioni alla Policy possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e/o genitori a docenti e/o 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 sottolineare il fatto che, nel momento stesso in cui 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 del codice penale);
- Induzione alla prostituzione minorile (art. 600bis);

- Pedopornografia (art. 600ter);
- Corruzione di minorenne (art. 609quinqies).

Per i reati sessuali la magistratura di norma procede su querela di parte; tuttavia, nei casi più gravi, si persegue d'ufficio ed in genere i reati verso minori sono tra questi ultimi.

Infrazioni dei genitori

Compito precipuo dei genitori è supportare gli insegnanti e il personale scolastico nel riconoscimento e nella costruzione di azioni di contrasto efficaci ai principali rischi rappresentati dalla navigazione in internet di utenti molto giovani e spesso poco accorti. Nel caso di infrazione si prevedono interventi, rapportati alla sua gravità, che vanno dalla semplice comunicazione del problema alla convocazione da parte dell'insegnante di classe o del Dirigente Scolastico.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

La policy richiede l'integrazione con l'inserimento delle seguenti norme:

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, il DSGA.

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 previa autorizzazione scritta del Responsabile di laboratorio. Si raccomanda, quindi, di verificare che il software installato rispetti 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 al Dirigente Scolastico.

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 contestualmente alla revisione del PTOF, a cura del Dirigente scolastico, dell'Animatore digitale e dei collaboratori del Dirigente, a seguito di verifica atta a constatare l'insorgenza di nuove necessità e la revisione di tecnologie esistenti.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

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

Azioni da svolgere nei prossimi 3 anni:

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per l'aggiornamento dell'ePolicy.
- Organizzare incontri per la consultazione degli studenti/studentesse e dei genitori sui temi dell'ePolicy per cui si evidenzia la necessità di aggiornare la regolamentazioni di azioni e comportamenti.

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 formazione del curricolo digitale non può non tener conto di quanto disposto dall'art. 5 della legge 20 agosto 2019 n. 92 (Introduzione dell'insegnamento scolastico dell'educazione civica) interamente dedicato alla "cittadinanza digitale" intesa come capacità di un individuo di avvalersi consapevolmente e responsabilmente dei mezzi di comunicazione virtuali.

Sono state individuate pertanto diverse aree tematiche relative alla Cittadinanza Digitale all'interno delle quali si approfondiscono diritti e doveri del Nuovi Nativi Digitali.

In occasione del **Safer Internet Day 2020** l'animatore digitale del nostro Istituto ha invitato tutti i docenti a condividere qualche momento della diretta con le classi, grazie alle LIM delle aule. Tutte le classi hanno avuto modo di venire a conoscenza dell'evento e quindi delle relative tematiche affrontate.

Tra gli accordi di Rete invece, l'Istituto ha scelto di aderire al progetto **#IONCADONELLARETE,** in collaborazione con il Dipartimento di Psicologia Dinamica e Clinica dell'Università Sapienza di Roma e con il Dipartimento di Sociologia e politiche Sociali dell'Università di Cassino e del Lazio meridionale.

Si tratta di un gioco a squadre che utilizza un Test on-line, per stimolare la curiosità degli adolescenti sui pericoli nascosti di un web, in grado di mutare senza preavviso in una trappola nella quale si può cadere senza riuscire a venirne fuori.

Dall'A.S. 2020/2021 tale progetto rientra tra i percorsi di PCTO.

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.

Le attività di formazione si svolgeranno su diversi livelli:

- formazione istituzionale, organizzata dal Miur secondo il PNSD, attraverso gli snodi formativi;
- formazione istituzionale in contrasto al bullismo, mediante interventi su classi individuate dalla scuola stessa, o interventi che vedono la presenza dell'intera comunità educante, compresi i genitori, o la formazione dei referenti di istituto;
- formazione specifica di Istituto, legata alle esigenza formative rilevate;
- partecipazione a progetti con la finalità di condividere materiale e tecniche di prevenzione e gestione di casi di bullismo.

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.

Al fine di promuovere la formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet, si prevedono momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi.

Uno delle prime proposte dei docenti del gruppo di lavori epolicy sarà proprio la fruizione dei Corsi proposti dalla piattaforma "Generazioni Connesse".

Inoltre sulla bacheca dell'IStituto dedicata saranno messi a disposizione per la condivisione:

- materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di internet;
- materiali informativi sulla sicurezza in internet per l'approfondimento personale, per le attività con gli studenti e gli incontri con i genitori;
- link a siti specializzati e contributi dal sito "Generazioni connesse";
- avvisi relativi a corsi di formazione/aggiornamneto sia interni che esterni all'Istituto.

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.

Da quando nel 2017 è stata approvata la Legge sul cyberbullismo, l'Istituto ha provveduto ad integrare nel "Patto di corresponsabilità" la parte relativa appunto al tema dell'uso delle tecnologie

digitali e dai rischi conseguenti. Tale Patto viene condiviso tramite il registro elettronico con le famiglie e durante i primi Consigli di Classe ne viene discusso il contenuto alla presenza di Rappresentanti di Genitori e Studenti.

Il presente documento di Epolicy sarà pubblicato sul sito e condiviso sulla bacheca di familgie e studenti, contestualmente al portala “Generazioni connesse” per consentire alle famiglie una piena conoscenza del regolamento sull’utilizzo delle nuove tecnologie all’interno dell’istituto e favorire un’attiva collaborazione con la scuola.

Il nostro piano d'azioni

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

- 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.

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

- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell’ambito dell’educazione alla cittadinanza digitale.
- 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.

Sul sito del nostro Istituto sono pubblicate, ai sensi dell'articolo 13 del Regolamento (UE) 2016/679, le informazioni sul trattamento dei dati personali che consultano il sito web.

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. In caso di attività di ampliamento dell'offerta formativa, organizzate in collaborazione con Enti esterni, viene richiesto preventivamente ai genitori il consenso informato alle riprese audio/ video e al loro eventuale utilizzo per scopi didattici, informativi e divulgativi anche tramite pubblicazione su siti web.

3.2 - Accesso ad Internet

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

Così recita l’art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le “misure riguardanti l’accesso a un’Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all’interno dell’Unione”.

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

modo che il “diritto a Internet” diventi una realtà, a partire dalla scuola”.

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

Il nostro Istituto, in entrambe le sedi, è dotato di una rete wi-fi , protetta da password in possesso esclusivo del Responsabile Tecnico della rete.

I docenti utilizzano quotidianamente i computer all'interno delle classi. Le operazioni di gestione, configurazione, backup e ripristino sono affidate ai tecnici interni presenti nell’Istituto.

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.

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 nostro Istituto è dotato di diversi strumenti per la comunicazione online, sia per quella esterna che per quella interna.

Per la **comunicazione esterna:**

- il sito web della scuola www.liceosianiaversa.edu.it, attraverso il quale vengono comunicate e promosse le attività portate avanti dall'Istituto (per raggiungere target esterni), ma vengono anche pubblicate le informazioni di servizio più importanti (chiusure straordinare, orari, ricevimenti, etc...);
- profilo facebook https://www.facebook.com/liceogiancarlosianiaversa, dove in particolare vengono diffuse le attività realizaate dai ragazzi e dall'Istituto su tematiche particolari (PCTO, visite guidate, giornate a tema,....).

Per la **comunicazione interna:**

- il registro elettronico per tutte le attività. Nell'ultimo periodo, causa emergenza sanitaria, ci

sono stati continui aggiormaneti anche nelel funzionalità delo stesso, e l'Animatore Digitale ha provveduto ad informare i Colleghi su tuttele potenzialità offerte dallo stesso;
- gruppi WhatsApp tra gruppi di docenti e per intero collegio;
- tutti i docenti dell'istituto possiedono una e-mail istituzionale del tipo: nome.cognome@liceosianiaversa.edu.it, attraverso la quale vengono inoltrate comunicazioni, vengono svolte attività didattiche nelle classi virtuali, si programmano appuntamneti e riunioni tramite un Calendario;
- gli studenti, per l'utilizzo delle attività didattiche in modalità Flipped e per la DaD sono dotati di un indirizzo di posta elettronica del tipo: st.cognome.nome@liceosianiaversa.edu.it. La dotazione di indirizzi di posta elettronica sia dei docenti che degli studenti appartiene alla piattaforma Google Suite for Education.

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.

Ormai lo smartphone è diventato uno strumento indispensabile a scuola. sia per docenti che per i studenti, sopratutto in quai casi, non molti, dove nelle aule non è presente la LIM e quindi bisogna ricorrere al dispositivi personali per poter svolgere almeno le attività essenziali (appello, voti, ...).

Come espresso nel Regolamento per gli studenti, i telefoni cellulari, non verranno utilizzati durante le lezioni scolastiche per bisogni propri e l'uso improprio viene sanzionato.

Il docente inoltre informerà inoltre gli alunni che l'utilizzo non consentito/non corretto dei dispositivi suddetti negli ambienti scolastici può configurarsi come violazione della privacy. È quindi perseguibile per legge, oltre che sanzionabile secondo il regolamento scolastico. Alunni con bisogni educativi speciali devono avere la possibilità di utilizzare in classe i propri dispositivi personali, pc e tablet compresi, come strumenti compensativi, anche con accesso a internet. Gli insegnanti di classe

avranno cura di vigilare sul corretto utilizzo di tali dispositivi.

BYOD letteralmente significa “porta il tuo dispositivo” ed è un’espressione che descrive quelle politiche aziendali che in tutto il mondo consentono agli impiegati di utilizzare i propri dispositivi personali in ambiente di lavoro.

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

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

dispositivi personali. Le tecnologie digitali devono essere funzionali a questa collaborazione. Lo scopo condiviso è promuovere la crescita di cittadini autonomi e responsabili.

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

Anche il progetto Generazioni Connesse, d'altra parte, va verso la responsabilizzazione di tutti i soggetti in gioco nel processo educativo e didattico dove l'utilizzo delle tecnologie e dei dispositivi anche personali va mediato e calibrato sviluppando un pensiero critico.

Laddove lo strumento viene utilizzato per integrare la didattica per attività in modalità BYOD, come previsto dal PNSD, si prevede che, con la condivisione della presente Policy, "le famiglie si assumono l'impegno di rispondere direttamente dell'operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone" a seguito di violazioni della presente policy".

Il nostro piano d'azioni

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

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte delpersonale Tecnico Amministrativo e dagli ATA
- 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 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 studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Organizzare incontri per la consultazione degli studenti/studentesse suindicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamentisull'uso dei dispositivi digitali personali

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

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

La sensibilizzazione costituisce il primo passo verso un cambiamento positivo, ma per far sì che l'intervento sia efficace, è importante che sia chiara l'azione verso cui i soggetti devono impegnarsi. Due sono gli aspetti che bisogna tenere in considerazione: la consapevolezza dello status quo; la motivazione al cambiamento. Per far sì che un intervento di sensibilizzazione sia efficace, è quindi importante fornire ai beneficiari informazioni chiare su quello che è lo stato attuale del tema che si vuole trattare (ad es. se si vuol trattare il tema del Cyberbullismo, sarà opportuno fornire informazioni su quali sono le caratteristiche del fenomeno e i dati rappresentativi). In questo modo gli utenti avranno tutte le informazioni necessarie per avere una fotografia chiara del contenuto che si sta trattando e del perché è necessario impegnarsi verso un cambiamento (motivazione al

cambiamento).

In sintesi, è opportuno tenere in considerazione i seguenti aspetti:

- spingere le persone a desiderare un cambiamento;
- porre in evidenza la possibilità di generare un cambiamento;
- individuare le azioni che consentono di produrre il cambiamento.

Un'attività di sensibilizzazione dovrebbe quindi fornire non solo le informazioni necessarie, ma anche illustrare le possibili soluzioni o comportamenti da adottare. Per prevenzione si intende un insieme molto ampio di strategie che coinvolgono le famiglie e le forze sociali che operano sul territorio al fine di mettere al proprio centro l'educazione formativa dei ragazzi. Nello specifico il nostro istituto attiverà una serie di misure volte a prevenire e contrastare bullismo e cyberbullismo: -integrare nel curricolo temi legati al corretto utilizzo delle TIC e di Internet; - progettare unità didattiche specifiche pianificate a livello di dipartimenti disciplinari; - supportare e implementare la competenza digitale in tutti i ragazzi all'interno delle materie curricolari.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

La legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", nell'art. 1, comma 2, definisce il cyberbullismo:

"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo".

La stessa legge e le relative **Linee di orientamento per la prevenzione e il contrasto del cyberbullismo** indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;

- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
    - Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
    - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Il cyberbullismo ("bullismo elettronico" o "bullismo in internet") è una forma di bullismo attuata attraverso l'uso dei Nuovi Media (dai cellulari a tutto ciò che si può connettere a internet). Come il bullismo tradizionale è una forma di prevaricazione e di oppressione reiterata nel tempo, perpetuata da una persona o da un gruppo di persone più potenti nei confronti di un'altra persona percepita come più debole.

Le caratteristiche tipiche del bullismo sono l'intenzionalità, la persistenza nel tempo, l'asimmetria di potere e la natura sociale del fenomeno (Olweus, 1996), ma nel cyberbullismo intervengono anche altri elementi, quali:

- L'impatto (viralità): la diffusione di materiale tramite internet è incontrollabile e non è possibile prevederne i limiti (anche se la situazione migliora, video e immagini potrebbero restare online.)
- La possibile anonimità: chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile
- L'assenza di confini spaziali: il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo dei suoi spazi-rifugio (è raggiungibile infatti anche a casa propria).
- L'assenza di limiti temporali: il cyberbullismo può avvenire a ogni ora del giorno e della notte. Sempre più spesso il cyberbullismo è collegato al bullismo tradizionale. Azioni di bullismo reale, ad esempio, possono essere fotografate o videoriprese, per poi essere pubblicate e diffuse sul web (social network, siti di foto-video sharing, email, blog, forum e chat).
- L'indebolimento dell'empatia: esistono cellule chiamate neuroni specchio che ci permettono di "leggere" gli altri quando li abbiamo di fronte, capirli e di provare emozioni simile a quelle che loro provano, proprio come se fossimo di fronte ad uno specchio. Quando le interazioni avvengono online la funzione speciale di questi neuroni viene meno.
- Il feedback non tangibile: il cyberbullo non vede in modo diretto le reazioni della vittima e, ancora una volta, ciò riduce fortemente l'empatia e il riconoscimento del danno provocato.

A tal proposito, il nostro Istituto con il progetto #IONONCADONELLARETE, ha invitato gli studenti a riflettere sul tema, proponendosi le seguenti finalità:

- creare una consapevolezza diffusa sulla presenza del bullismo all'interno delle Istituzioni Scolastiche;
- accrescere le capacità di intervento, sia in ottica preventiva, sia di gestione degli episodi già

verificatisi;
- approfondire la conoscenza delle tecnologie digitali, del funzionamento del web, delle dinamiche dei social network;
- promuovere negli studenti comportamenti empatici e pro sociali;
- promuovere negli studenti buone prassi comportamentali;
- promuovere la sicurezza in Rete degli studenti, perché acquisiscano le competenze necessarie all'esercizio di una cittadinanza digitale consapevole;
- realizzare un'alfabetizzazione emotiva, individuando nell'analfabetismo emotivo, accresciuto dai mezzi tecnologici, la causa prima di atteggiamenti sociali violenti e intenzionali, di natura sia fisica che psicologica;
- promuovere la costruzione di un ambiente emotivamente sano, perché esso costituisce un terreno fertile per l' apprendimento e la socializzazione, sposando a pieno il concetto di "intelligenza emotiva" (Goleman, 1990) che vuole occuparsi prima delle emozioni dei ragazzi e quindi poi delle loro abilità e talenti.

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.

Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono quindi un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete. Occorre in tal senso fornire ai più giovani gli strumenti necessari per decostruire

gli stereotipi su cui spesso si fondano forme di hate speech, e promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network. Si potrebbe, quindi, pensare ad attività di analisi e produzione mediale, finalizzate soprattutto a: 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

---

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?

Il nostro Istituto promuoverà sicuramente percorsi sul benessere digitale, data la rilevante diffusione di tale fenomeno.

Infatti la dipendenza da Internet, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica che deve attenzionare il fenomeno e fornire gli strumenti agli studenti e alle studentesse affinché questi siano consapevoli dei rischi che comporta l'iperconnessione.

La S.I.I.Pa.C., la Società Italiana Intervento Patologie Compulsive, definisce la dipendenza da Internet come progressivo e totale assorbimento del soggetto alla Rete; di seguito alcune caratteristiche specifiche:

- Dominanza. L'attività domina i pensieri ed il comportamento del soggetto, assumendo un valore primario tra tutti gli interessi.
- Alterazioni del tono dell'umore. L'inizio dell'attività provoca cambiamenti nel tono dell'umore. Il soggetto prova un aumento d'eccitazione o maggiore rilassatezza come diretta conseguenza dell'incontro con l'oggetto della dipendenza.
- Conflitto. Conflitti inter-personali tra il soggetto e coloro che gli sono vicini, conflitti intrapersonali interni a se stesso, a causa del comportamento dipendente.
- Ricaduta. Tendenza a ricominciare l'attività dopo averla interrotta.

I segnali patologici di questo che viene descritto come "un vero e proprio abuso della tecnologia", anche denominato "Internet Addiction Disorder" (I.A.D. coniato dallo psichiatra Ivan Goldberg 1996), sono specifici così come accade per le altre dipendenze più "tradizionali". In particolare, si hanno: la tolleranza ossia quando vi è un crescente bisogno di aumentare il tempo su internet e

l'astinenza quando, cioè, vi è l'interruzione o la riduzione dell'uso della Rete che comporta ansia, agitazione psicomotoria, fantasie, pensieri ossessivi (malessere psichico e/o fisico che si manifesta quando s'interrompe o si riduce il comportamento). Tutto questo ha ripercussioni sulla sfera delle relazioni interpersonali che diventano via via più povere e alle quali si preferisce il mondo virtuale, con alterazioni dell'umore e della percezione del tempo.

Di seguito i sintomi che devono essere presenti (per un arco di tempo di almeno un anno):

1. il giocatore è assorbito totalmente dal gioco;

2. il giocatore è preoccupato e ossessionato dal gioco;

3. il gioco consente alla persona di sfuggire alla realtà con la sperimentazione di emozioni più piacevoli;

4. il giocatore manifesta sempre di più l'impulso di giocare e di sperimentare emozioni positive;

5. il giocatore sente di dover dedicare più tempo ai giochi;

6. il giocatore se non può giocare manifesta ansia, depressione e irritabilità;

7. può emergere un ritiro sociale;

8. il giocatore, anche se comprende la gravità della situazione e sospende di giocare comunque non riesce a interrompere del tutto;

9. il giocatore mente agli altri sull'utilizzo che fa dei giochi on line;

10. il giocatore ha perso o mette a rischio relazioni o opportunità a causa dei giochi su Internet o ha perso interesse verso attività nella vita reale.

La scuola, anche in questo caso, ha la possibilità di fare formazione e di indicare strategie per un uso più consapevole delle tecnologie per favorire il "benessere digitale", cioè la capacità di creare e mantenere una relazione sana con la tecnologia. La tecnologia infatti ha modificato gli ambienti che viviamo e ha un impatto sulla qualità della vita. Gli elementi che contribuiscono al benessere digitale sono: la ricerca di equilibrio nelle relazioni anche online l'uso degli strumenti digitali per il raggiungimento di obiettivi personali la capacità di interagire negli ambienti digitali in modo sicuro e responsabile la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche) Se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi. Strutturare regole condivise e stipulare con loro una sorta di "patto" d'aula e, infine, proporre delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d'aula (Es. adoperando la LIM o il dispositivo personale). È importante, quindi, non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli/lle studenti e delle studentesse, stabilendo chiare e semplici regole di utilizzo.

4.5 - Sexting

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

Il sexting (abbreviazione di sex – sesso e texting – messaggiare, inviare messaggi) indica l’invio e/o la ricezione di contenuti (video o immagini) sessualmente espliciti che ritraggono se stessi o gli altri.

Questi contenuti possono diventare materiale di ricatto assumendo la forma di “revenge porn” letteralmente “vendetta porno” fenomeno quest’ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l’altra parte (la Legge 19 luglio 2019 n. 69, all’articolo 10 ha introdotto in Italia il reato di revenge porn, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti. Si veda l’articolo 612 ter del codice penale rubricato “Diffusione illecita di immagini o video sessualmente espliciti”. Tra le caratteristiche del fenomeno vi sono principalmente:

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

La consapevolezza, o comunque la sola idea di diffusione di contenuti personali, si replica nel tempo e può finire con il danneggiare, sia in termini psicologici che sociali, sia il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che hanno contribuito a diffonderla. Due agiti, quindi, che sono fra loro strettamente legati e che rappresentano veri e propri comportamenti criminali i quali hanno ripercussioni negative sulla vittima in termini di autostima, di credibilità, di reputazione sociale off e on line. A ciò si associano altri comportamenti a rischio, di tipo sessuale ma anche riferibili ad abuso di sostanze o di alcool. I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell’altro/i e depressione.

4.6 - Adescamento online

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

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

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

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

Il nostro Istituto promuoverà incontri di:

- sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione;
- prevenzione dell'adescamento in rete;
- buone prassi qualora si venga a conoscenza di casi simili, educando l'utenza a saperne valutare la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.

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.

Al di là delle interpretazioni della giurisprudenza in merito, il fenomeno dei sexting richiede più utilmente di porre l'attenzione sulla necessità della prevenzione: i più giovani devono acquisire quelle competenze in grado di orientarli e guidarli nelle loro scelte anche online; per questo motivo l'educazione, compresa l'educazione all'affettività, riveste un ruolo fondamentale. In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere. Ad esempio, non è utile diffondere tra i bambini e le bambine più piccoli/e l'uso di servizi come le hotline, sia perché in caso di visione accidentale di materiale pedopornografico è opportuno che bambini/e e ragazzi/e possano parlarne con gli adulti di riferimento per la migliore risposta possibile, sia perché si potrebbe incentivare la ricerca proattiva, che comunque è vietata dalla legge italiana, per minori e per adulti. Risulta utilissima l'attività educativa sull'affettività e le relazioni, sottolineando sempre la necessità di rivolgersi ad un adulto quando qualcosa online mette a disagio. La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Su tale problematica il nostro Istituto si propone di realizzare attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse.

Il nostro piano d'azioni

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

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

☐ Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

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

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 ai docenti e agli studenti/studentesse.

☐ Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

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

☐ Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

- **Cyberbullismo**: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/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.

Le procedure indicate in questa sezione si riferiscono, oltre a quelle sopra indicate, legate ad un utilizzo scorretto delle TIC (Tecnologie dell'Informazione e della Comunicazione), anche a tutte le azioni da mettere in pratica per la presa in carico e relativa gestione delle situazioni di bullismo e cyberbullismo.

IL TEAM DELL'EMERGENZA Con apposito atto di nomina, il Dirigente Scolastico individua un gruppo o team specializzato con competenze, responsabilità, tempi e modalità d'azione specifiche, per la gestione dei casi. Il team sarà coordinato dal referente per il contrasto del bullismo e del cyberbullismo. Il team è composto da 3 o più persone, tra insegnanti con competenze trasversali e figure professionali diverse che lavorano nella scuola (psicologo o psicopedagogista), formate sul tema delle azioni indicate contro il bullismo/cyberbullismo.

Il Team per le emergenze, osservando quanto descritto nel Capitolo 1 del presente documento in quanto a ruoli e responsabilità, agisce in quanto a: responsabilità della presa in carico conduzione della valutazione responsabilità della decisione relativa alla tipologia di intervento implementare alcuni interventi monitoraggio del caso nel tempo responsabilità della decisione relativa all'andamento del caso nel tempo stretta connessione con i servizi del territorio

---

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.

L'Istituto, oltre al dovere di sorveglianza degli insegnanti (*culpa in vigilando*) adotta il presente Protocollo di Gestione dell'emergenza che, accogliendo gli strumenti di segnalazione sopra indicati, definisce le procedure da seguire una volta che è avvenuto un presunto episodio di bullismo/cyberbullismo e vittimizzazione e prevede 4 passi fondamentali:

1. Prima segnalazione

2. Valutazione approfondita

3. Scelta dell'intervento e della gestione del caso

4. Monitoraggio

Lo schema allegato "*Procedura per caso presunto bullismo e vittimizzazione a scuola*" rappresenta graficamente il Protocollo di gestione dell'emergenza.

Il Protocollo di Gestione dell'emergenza comprende, in quanto azioni propedeutiche alla redazione della SCHEDA DI PRIMA SEGNALAZIONE, gli schemi allegati al presente capitolo e che rappresentano rispettivamente:

- Procedure interne in caso di Cyberbullismo Procedure interne in caso di Sexting
- Procedure interne in caso di adescamento on line
- Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola.

FASE 1 – ACCOGLIERE LA SEGNALAZIONE DI UN CASO PRESUNTO DI BULLISMO

Lo scopo di questa fase è quella di attivare un processo di attenzione e di successive valutazioni relative ad un presunto caso di bullismo/cyberbullismo. La segnalazione può farla chiunque: vittima, genitori, testimoni, docenti, personale ATA. Accogliere la segnalazione non significa denunciare bensì prendere in carico una situazione che necessita di approfondimenti ed escludere che un caso di sofferenza non venga considerato perché sottovalutato o ritenuto di poca importanza. Viene redatta utilizzando l'apposito modulo "SCHEDA DI PRIMA SEGNALAZIONE".

La scheda, elaborata in modo semplice e funzionale alla raccolta di dati essenziali, sarà diffusa in modalità cartacea nei luoghi a cui hanno accesso tutti coloro che possano avere necessità di compilarla. Sarà altresì disponibile in modalità digitale nell'apposita sezione sul sito istituzionale dell'Istituto. Uno o più componenti, appositamente designati, del team d'emergenza, raccolgono le schede di prima segnalazione per attivarne la relativa gestione e monitoraggio.

FASE 2 – VALUTAZIONE APPROFONDITA

Lo scopo di questa fase è valutare esattamente la tipologia e la gravità dei fatti per poter definire un intervento. Viene condotta dal team dell'emergenza insieme a chi ha fatto la prima segnalazione. E' importante che questa fase venga attivata entro almeno 2 giorni da quando è stata presentata la prima segnalazione affinché con l'acquisizione di ulteriori informazioni si possano prendere decisioni circa le modalità di gestione del caso.

Il componente del team che prenderà in carico il caso, attraverso degli incontri e dei colloqui appositamente strutturati, redigerà lo screening utilizzando il modulo "VALUTAZIONE APPROFONDITA DEI CASI DI BULLISMO E VITTIMIZZAZIONE"

FASE 3 – GESTIONE DEL CASO

In base alle informazioni acquisite si delinea il LIVELLOD DI RISCHIO DI BULLISMO E VITTIMIZZAZIONE con conseguente grado di priorità dell'intervento:

- Livello CODICE VERDE = Situazione da monitorare con interventi preventivi nella classe
- Livello CODICE GIALLO = Interventi indicati e strutturati a scuola e in sequenza coinvolgimento della rete se non ci sono risultati
- LIVELLO CODICE ROSSO = Interventi di emergenza con supporto della rete

In base al livello verranno poi delineate le azioni da intraprendere e, il team dell'emergenza, ha il compito di coinvolgere le altre figure che supporteranno la realizzazione dell'intervento/degli interventi (es. i docenti della classe per l'intervento educativo con la classe).

Gli interventi sono di seguito classificati:

1. **Approccio educativo con la classe**, in cui vengono coinvolti gli insegnanti della classe per affrontare direttamente l'accaduto e sensibilizzare rrispetto al fenomeno generale

2. **Intervento individuale**, con il bullo e la vittima, in cui è richiesto il supporto di un docente con competenze trasversali e, ove possibile, del psicologo della scuola

3. **Gestione della relazione**, secondo l'approccio della Mediazione o dell'Interesse condiviso, a seconda del caso da trattare

4. **Coinvolgimento della famiglia**, che può essere realizzato anche in momenti diversi in funzione della specifica situazione, delle indicazioni del DS, dell'obiettivo del team, o del docente referente della scuola e delle capacità di quest'ultima di poter avviare una prima gestione del caso. Se i genitori sono coinvolti nella fase di valutazione iniziale o hanno segnalato loro stessi il problema, è importante impostare fin da subito una collaborazione attiva tra scuola e famiglia per la soluzione

del caso. L'art. 5 della L.71/2017 sancisce precise circostanze in presenza delle quali il DS provvede a informare la famiglia.

5. **Supporto intensivo a lungo termine e di rete**, da richiedere nel caso in cui gli atti di bullismo siano di una gravità elevata la sofferenza della vittima è molto elevata i comportamenti aggressivi e a rischio dei bulli sono considerevoli.

Va evidenziato che gli insegnanti, in quanto incaricati di pubblico servizio, hanno obbligo di denuncia qualora vengano a conoscenza di reati perseguibili d'ufficio. Nella scheda di approfondimento "I PRINCIPALI REATI PROCEDIBILI D'UFFICIO" ne sono indicati i principali. Non ci sono tuttavia reati specifici che descrivono comportamenti illeciti tenuti on-line e si deve quindi fare riferimento ai reati sopra elencati. Ad esempio i comportamenti come il Cyberbullismo e il Sexting vanno valutati caso per caso in quanto possono includere uno o più dei reati perseguibili d'ufficio elencati nella scheda di approfondimento. Va altresì evidenziato che 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.

Oltre al team dell'emergenza, sono disponibili 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.

FASE 4 – MONITORAGGIO

Il monitoraggio è una fase importante del processo che permette al team per la gestione delle emergenze di verificare la presenza di cambiamenti a seguito dell'intervento/degli interventi messi in atto: lo strumento utile allo scopo è la "**SCHEDA DI MONITORAGGIO".**

A breve termine (entro una/due settimane) permette di capire se la situazione è migliorata o se sono necessarie azioni aggiuntive; a lungo termine (dopo circa 1 mese dalla redazione della Scheda di Monitoraggio) permette di verificare se il cambiamento ottenuto a seguito dell'intervento si mantiene nel tempo. La fase di monitoraggio include anche la rilevazione di tutti gli episodi di bullismo/cyberbullismo gestiti in un apposito DIARIO DI BORDO, redatto dal referente d'istituto per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo.

RUOLI, COMPITI E FUNZIONI: CHI FA COSA.

Il **docente** e Il consiglio di Classe, dopo essere stati allertati da un genitore, un alunno o da uno dei componenti della comunità scolastica, contattano prontamente il Dirigente Scolastico per comunicargli l'accaduto e d'accordo con la dirigenza vengono stabiliti tempi e modi di comunicazione alla famiglia e i successivi passi da intraprendere.

In particolare, presenza di sospetto relativo a un episodio di cyberbullismo, basato su testimonianza diretta o diretta visione di prodotti informatici di tipo denigratorio o usati a tal fine (foto, post, video,

...), il docente, venuto a conoscenza dei fatti nell'esercizio delle proprie funzioni, in qualità di Pubblico Ufficiale (art. 357 c.p. e art. 331 c.p.p.), relaziona al Dirigente Scolastico per iscritto, avendo cura di far protocollare la propria segnalazione, da inoltrarsi preferibilmente a mano in busta chiusa. Il Dirigente deve comunicare per iscritto al docente l'avvenuta trasmissione all'autorità competente. Qualora ciò non avvenisse entro i due
giorni lavorativi successivi al protocollo, il docente stesso dovrà inoltrare la segnalazione.

Nel caso in cui un docente sospetti che stia avvenendo qualcosa riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online fra gli studenti e le studentesse, informa i colleghi titolari sulla classe e osservano e monitorano il clima di classe e le dinamiche relazionali.

Nel caso in cui un docente abbia certezza del fatto che siano avvenuti casi riferibili a bullismo e/o cyberbullismo, sexting o adescamento online, invece, viene avvisato il Dirigente Scolastico che può convocare il Consiglio di Classe e, in base alla gravità della situazione, stabilisce in che tempi e con che modalità avvisare le famiglie degli studenti e delle studentesse direttamente coinvolti. Se lo ritiene opportuno, invita i genitori a rivolgersi allo sportello psico-pedagogico.

In caso sia individuata la **vittima**, il Dirigente Scolastico o, su delega, il Vicario e/o il Secondo Collaboratore, e/o il coordinatore di classe, e/o il referente per il bullismo o cyberbullismo, deve convocare i genitori (o chi esercita la responsabilità genitoriale) e informarli dei fatti, eventualmente con il supporto degli esperti dello sportello di ascolto. La convocazione dei genitori non deve essere fatta per i reati di sexting, pedopornografia o per altri reati in cui sia possibile che la vulnerabilità del minore nasca all'interno del nucleo familiare.

A seconda della situazione e delle valutazioni effettuate, **il caso può essere segnalato alle autorità competent**i e si può richiedere, se ritenuto opportuno, il sostegno dei servizi e delle associazioni territoriali.

Gli **studenti,** che vivano in prima persona o come testimoni situazioni problematiche, possono rivolgersi ai docenti di classe, al coordinatore di classe, al Dirigente Scolastico, al referente per il contrasto del bullismo e del cyberbullismo, al referente dello sportello d'ascolto e/o agli psicologi operanti all'interno dell'Istituto, ai servizi di consulenza on-line (sportellostudenti@diregiovani.it), al referente Scuole Sicure del Commissariato Esquilino di Roma, a qualsiasi commissariato di P.S., al commissariato on-line(https://www.commissariatodips.it/), alla Polizia Postale, all'Arma dei Carabinieri. Inoltre, gli studenti possono inviare la propria segnalazione, anche in forma anonima, tramite l'applicazione You Pol della Polizia di Stato (https://www.poliziadistato.it/statics/40/presentazione_youpol_-esserci.pdf.pdf). In particolare, i minori che ritengano che determinanti contenuti a loro riferiti e diffusi per via telematica (foto e/o video imbarazzanti e/o offensivi, pagine web e/o post sui social network in cui si è vittime di minacce e/o offese e/o insulti, ecc.) siano atti di cyberbullismo, ne possono richiedere l'oscuramento, la rimozione o il blocco. Le richieste vanno inviate altitolare del trattamento o al gestore del sito o del social media dove sono pubblicati i contenuti ritenuti atti di cyberbullismo. L'istanza può essere inoltrata direttamente dal minore, se ha più di 14 anni, oppure da chi esercita la responsabilità genitoriale. Nel caso la richiesta non venga soddisfatta, ci si può rivolgere al Garante per la protezione dei datipersonali, che, entro 48 ore, provvede in merito alla segnalazione (legge n 71/2017).

Per inoltrare segnalazioni si può utilizzare il modello scaricabile sul sito www.garanteprivacy.it/cyberbullismo, inviandolo via e mail a cyberbullismo@gpdp.it.

Gli **psicologi** operanti all'interno dell'Istituto scolastico, gli addetti del personale ATA, gli esperti esterni coinvolti in attività di docenza per attività dell'Istituto (progetti, PCTO, corsi...), in sede o fuori sede, ricoprono il ruolo di Operatori Incaricati di Pubblico Servizio(art.358 c.p.) e come tali sono obbligati a denunciare e o segnalare i fatti appartenenti alletipologie sopradescritte, di cui sono informati per testimonianza diretta o visione diretta dimateriale che rientri nelle categorie di reati precedentemente indicati. Pertanto, sono tenutia mettere in atto le procedure contenute nei precedenti paragrafi, comunicando, inoltre, per iscritto, al docente con cui abitualmente hanno contatti (referente di progetto, coordinatoredi classe, docente della classe,...), i fatti di cui sono venuti a conoscenza e l'avvenutasegnalazione al Dirigente Scolastico e/o all'autorità di P.S. e/o all'autorità giudiziaria.

Il **consiglio di classe** a cui appartenga lo studente o il gruppo di studenti coinvolto nei fatti, previa informativa da parte del titolare della segnalazione/denuncia o da parte del Dirigente Scolastico, attiva percorsi di informazione, prevenzione e sensibilizzazione, avvalendosi, segiudicato opportuno, del supporto di esperti esterni quali psicologi, servizi sociali, forze dell'ordine, Polizia Postale, ecc. E' fondamentale che venga rispettato il segreto d'ufficio sull'identità dei soggetti implicati, indipendentemente dal loro ruolo.

Il consiglio di classe e, aseconda della gravità della violazione, il Consiglio d'Istituto valutano l'eventuale erogazione di provvedimenti o sanzioni disciplinari nelle sedi, nelle modalità e con le finalità previste dalRegolamento d'Istituto e dallo Statuto degli Studenti e delle Studentesse.
In tutte queste procedure, gli studenti, le famiglie, il personale ATA, gli esperti esterni, idocenti e il Dirigente Scolastico possono avvalersi della figura del **referente per il contrastoal bullismo e al cyberbullismo.**

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.

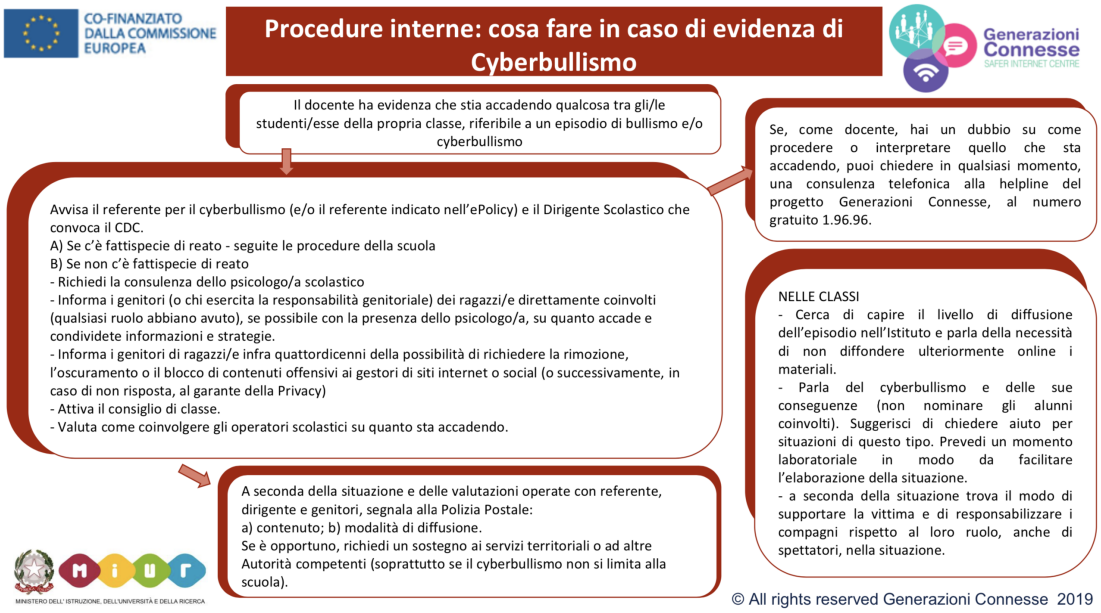
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **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.

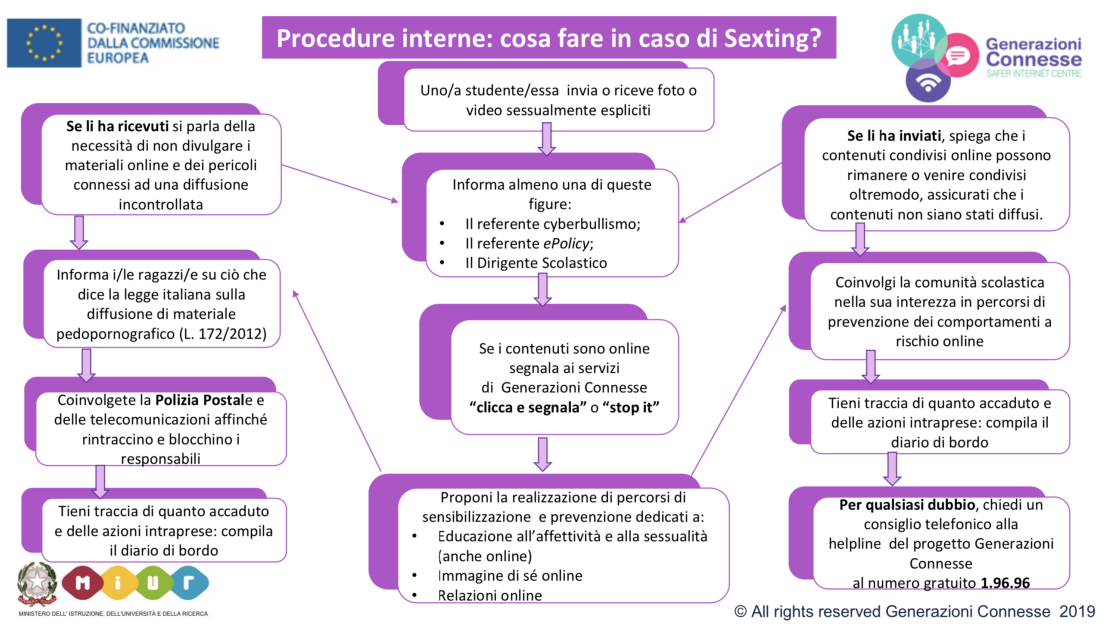
Nell'ambito della fase 3, ove si renda necessario il supporto intensivo di lungo termine e di rete, per individuare a chi rivolgersi e decidere quale agenzia contattare, il team dell'emergenza redige insieme al DS il modulo "INTERVENTO DI RETE CON IL TERRITORIO" utilizzando il Vademecum/guida operativa (allegato al presente documento) realizzato nell'ambito del progetto Generazioni Connesse SIC III – *Safer Internet Centre Italia* in cui è compresa la lista di servizi e istituzioni di cui sono forniti indirizzi e riferimenti telefonici, con una suddivisione regionale, per reperire risorse e supporto nei casi di bullismo e cyberbullismo.

5.4. - Allegati con le procedure

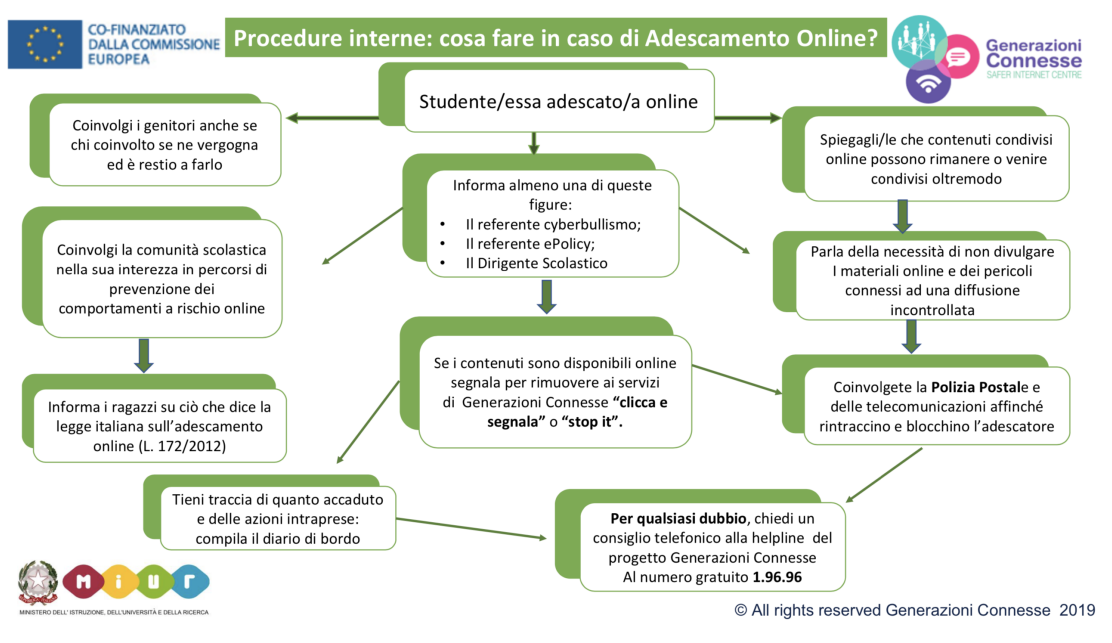
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



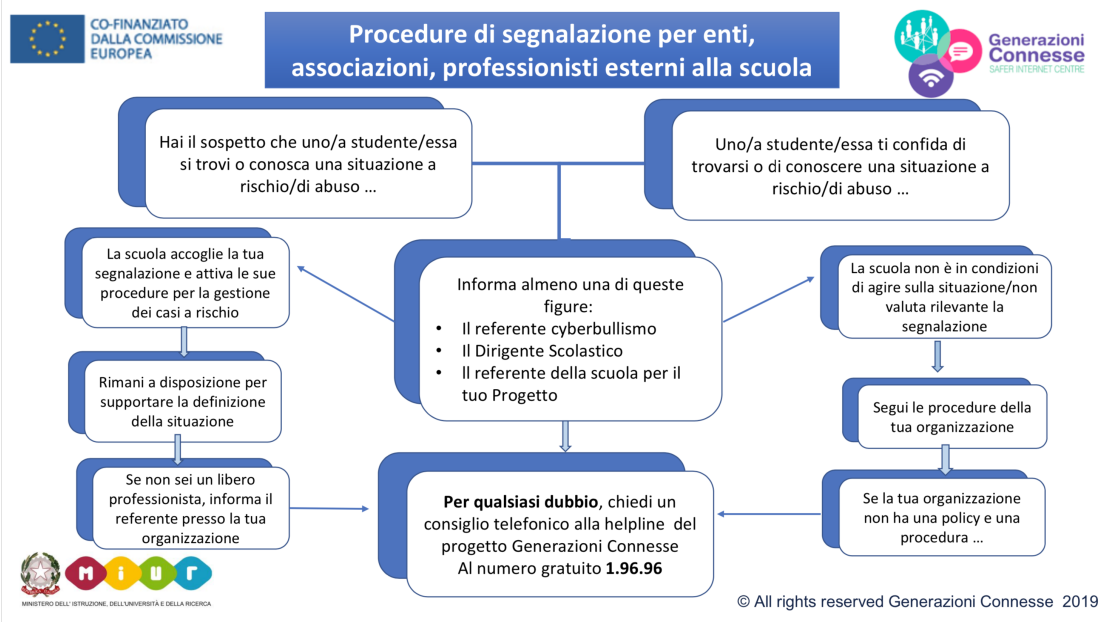
Procedure interne: cosa fare in caso di sexting?



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

Oltre agli schemi di procedura sopra indicati, che sono parte integrante del Protocollo di Gestione dell'Emergenza elaborato dall'Istituto, si procederà ad elaborare tutta la modulistica e le schede di approfondimento necessarie alla corretta attuazione delle procedure::

- Schema "Procedura per caso presunto bullismo e vittimizzazione a scuola""
- Modulo "SCHEDA DI PRIMA SEGNALAZIONE"
- Modulo "VALUTAZIONE APPROFONDITA DEI CASI DI BULLISMO E VITTIMIZZAZIONE"
- Modulo "SCHEDA DI MONITORAGGIO"
- Modulo "INTERVENTO DI RETE CON IL TERRITORIO" "VADEMECUM – Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzi delle tecnologie digitali da parte dei più giovani" realizzato nell'ambito del progetto Generazioni Connesse SIC III – Safer Internet Centre Italia
- Diario di bordo
- Scheda di approfondimento " I PRINCIPALI REATI PROCEDIBILI D'UFFICIO"

Il nostro piano d'azioni

(PRIMO ANNO)

- Ridefinizione del Regolamento d'Istituto nell'ottica dell'E-Policy.
- Organizzazione lancio del Protocollo di Emergenza rivolto a docenti, studenti/esse, famiglie.
- Creazione sul sito di una sezione dedicata alle procedure di segnalazione di violazione e alla modulistica specifica, con indicazione dei principali Enti e Servizi a cui rivolgersi per assistenza e tutela;

(TRIENNIO)

- Riformulazione del documento di E-policy per l'implementazione delle problematiche relative al bullismo basato sul pregiudizio (etnico, omofobico, verso la disabilità);
- Organizzazione incontri di formazione rivolto ai docenti e ai genitori sulle tecniche di gestione della relazione, ascolto attivo, comunicazione non verbale;
- Organizzazione incontri di formazione rivolto agli studenti sulle procedure di segnalazione di violazione e alla modulistica specifica, con indicazione dei principali Enti e Servizi a cui rivolgersi per assistenza e tutela