Documento di ePolicy

FGPC15000C

LICEO "BONGHI-ROSMINI"

VIALE FERROVIA 19 - 71036 - LUCERA - FOGGIA (FG)

Prof. Matteo Capra

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 daparte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'e-Policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

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

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

Argomenti del Documento

Perché è importante dotarsi di una E-policy?

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccioalla 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 Liceo "Bonghi-Rosmini", preso atto del diffuso utilizzo dell'ICT nella comunità di riferimento, accoglie l'istanza di dotarsi di una E-policy quale strumento operativo di riferimento per tutta la comunità educante in ordine ad un uso consapevole, critico ed efficace dell'ICT (TIC). Il documento elaborato, in collaborazione con il Safer Internet Centre, nell'ambito del Progetto "Generazioni Connesse" vuole coinvolgere tutte le componenti della Comunità scolastica: il personale della scuola, gli studenti e le famiglie.

L'Istituto ha redatto, nell'a.s. 2021-2022, la presente e-Policy in conformità con le "Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e cyberbullismo" emanate dal MIUR in collaborazione con il Safer Internet Center (SIC) per l'Italia, progetto co-finanziato dalla Commissione Europea nell'ambito del programma "Connecting Europe Facility" (CEF) - Telecom, con l'obiettivo di diffondere campagne di sensibilizzazione, promuovere azioni, risorse e servizi per un uso consapevole e responsabile delle tecnologie digitali e per la segnalazione delle problematiche connesse.

Il documento di E-Policy ha lo scopo di informare tutta la comunità educante circa l'uso corretto e responsabile della rete e i rischi connessi a quest'ultima, in tutti i momenti che coinvolgono le attività didattiche.

La E-Policy, inoltre, potrà costituire un supporto e fornire alcune linee guida per l'organizzazione dell'insegnamento di Educazione civica.

Nella stesura della E-Policy e nella definizione e attuazione delle procedure che questa prevede, oltre all'intera comunità scolastica, risultano principalmente coinvolti:

- Il Dirigente Scolastico, prof. Matteo Capra
- Il Referente del Contrasto al bullismo e cyberbullismo, prof.ssa Maria Angela Mendilicchio
- Il Team a supporto del Referente, proff. Antonietta Caserio, Luisa Castriota, Rosanna Criasia, Matteo De Mutiis, Simona Mariani, Marco Maruotti, Ilaria Pagano, Rita Testa
- L'animatore digitale, prof. Matteo De Mutiis e relativo team

Il presente Documento è parte integrante del PTOF e le azioni sottoscritte costituiscono indicazioni e buone prassi di azione e prevenzione in materia di bullismo e cyberbullismo.

1.2 - Ruoli e responsabilità

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

Il Dirigente Scolastico

- garantisce la formazione del personale docente e non docente sulla sicurezza e sulla prevenzione online
- controlla e vigila su fenomeni di hacking ai danni delle reti e dei computer dell'Istituto, nonché delle piattaforme utilizzate per la didattica e per la gestione dei dati amministrativi
- promuove la cultura della sicurezza online favorendo iniziative di formazione e prevenzione del fenomeno del cyberbullismo
- interviene nei casi più gravi di bullismo, cyberbullismo e uso improprio delle tecnologie digitali.

L'Animatore Digitale

- offre alla comunità scolastica il proprio supporto per quanto concerne gli aspetti tecnicoinformatici
- promuove percorsi di formazione interna per la scuola al fine di garantire lo sviluppo delle competenze digitali nell'ambito dell'Educazione civica
- promuove l'adesione ai bandi relativi allo sviluppo delle competenze digitali e si impegna nelle relative attività di progettazione e di realizzazione
- rileva le problematiche connesse all'utilizzo delle TIC affinché gli utenti autorizzati accedano alla rete della scuola tramite password
- supporta le attività del personale tecnico e amministrativo in relazione all'utilizzo delle tecnologie informatiche
- favorisce la dematerializzazione delle attività relative alla didattica e l'informatizzazione di parte delle comunicazioni scuola-famiglia
- interagisce e coopera con il DS, con il DSGA, con le Funzioni Strumentali d'Istituto e con il referente interno per il sito WEB per le tematiche di sua competenza.

Il Referente bullismo e cyberbullismo

- coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo, avvalendosi della cooperazione del Team Bullismo e Cyberbullismo, delle forze di Polizia, delle associazioni e dei centri di aggregazione giovanile del territorio
- coinvolge nei percorsi di formazione tutte le componenti della comunità scolastica (personale docente e non docente, studenti, genitori).

I Docenti

- integrano il curriculum della disciplina promuovendo l'uso delle TIC, nel rispetto della libertà d'insegnamento accompagnano e supportano gli studenti nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM e di altri dispositivi
- segnalano, in quanto Pubblici Ufficiali, al Dirigente Scolastico eventuali problematiche o casi di violenza e abuso online in cui siano coinvolti gli studenti, nel momento in cui ne vengano a conoscenza.

Il Personale Amministrativo, Tecnico e Ausiliario (ATA)

- garantisce supporto tecnico a studenti e docenti nei laboratori che prevedono l'uso della LIM e di altri dispositivi
- segnala, in qualità di Incaricato di Pubblico Servizio, comportamenti non adeguati nell'uso delle TIC ed episodi di bullismo e di cyberbullismo, nel momento in cui ne venga a conoscenza
- è coinvolto nelle attività di formazione e di autoformazione in tema di bullismo e cyberbullismo e uso responsabile della rete.

Gli Studenti e le Studentesse

- utilizzano le tecnologie digitali all'interno di percorsi formativi coerenti con gli obiettivi didattici ed educativi definiti dal Collegio Docenti
- imparano a tutelare se stessi e i propri compagni dai rischi online
- partecipano con senso di responsabilità alle iniziative e ai progetti di formazione proposti dalla scuola circa l'uso della rete e delle TIC.

I Genitori

- si impegnano a relazionarsi in maniera costruttiva con i docenti e ad agire in continuità con l'Istituto scolastico nella promozione e nell'educazione all'uso consapevole delle TIC e della rete, nonché all'uso responsabile dei device personali
- controllano e vigilano sulle attività svolte dai propri figli sui social network, leggono, accettano e condividono, all'atto dell'iscrizione, la E-policy dell'Istituto.

A conclusione di questa sezione, si ribadisce la corresponsabilità educativa e formativa che riguarda sia il personale della scuola che i genitori nel percorso di crescita degli studenti e delle studentesse.

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, Legge15 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 stabilito 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).

Le **organizzazioni/associazioni extrascolastiche** e gli **esperti esterni** chiamati, a vario titolo, alla realizzazione di progetti ed attività educative, sul breve o/e lungo periodo, dovranno prendere atto di quanto stilato nell' ePolicy del Liceo "Bonghi- Rosmini" e sottoscrivere un'informativa sintetica del documento in questione. I suddetti soggetti sono tenuti a:

- prendere visione della politica dell'Istituto riguardo all'uso consapevole e responsabile della rete e delle TIC
- promuovere la sicurezza online durante le attività di cui sono titolari
- segnalare ai docenti preposti e al Dirigente Scolastico eventuali comportamenti problema o casi di abuso nell'utilizzo della rete e delle TIC.

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

Il documento di ePolicy 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'ePolicy 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.

Nella prima riunione del Collegio Docenti, successiva alla redazione dell'ePolicy, si darà ampia diffusione al redatto documento per condividerlo e trarre spunti utili per il miglioramento. In una successiva riunione del Collegio Docenti se ne curerà l'approvazione da parte dello stesso e del Consiglio di Istituto.

Ai coordinatori di classe si fornirà copia del documento per la condivisione con gli studenti e studentesse delle loro classi. Inoltre, se ne curerà l'inserimento sul sito istituzionale nella sezione "Generazioni connesse-documento e-Policy" della scuola. Espliciti riferimenti all'E-policy verranno inseriti nel Patto di corresponsabilità, per darne comunicazione alle famiglie.

Sintetica informativa sull' e-Policy, con relativa procedura di segnalazione, verrà fornita ai soggetti esterni che erogano attività educative nell'Istituto.

1.5 - Gestione delle infrazioni alla ePolicy

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

Condotte sanzionabili

Oltre a quanto espressamente indicato nel Regolamento di Istituto, si segnalano le seguenti condotte inappropriate correlate all'uso delle TIC:

- condivisione online di immagini o video di compagni/e senza il loro consenso
- condivisione online di immagini o video di docenti senza il loro consenso
- condivisione online di immagini o video di compagni/e che li ritraggono in pose offensive e denigratorie
- condivisione di scatti intimi e a sfondo sessuale
- condivisione di dati personali altrui
- invio di immagini o video volti all'esclusione di compagni/e
- utilizzo di linguaggio denigratorio in una chat con lo scopo di escludere un compagno dal gruppo
- diffamazione di docenti o collaboratori scolastici attraverso social o app di messaggistica istantanea
- collegamenti a siti web inadeguati durante la permanenza a scuola
- incitamento all'odio nei confronti di un compagno o di un piccolo gruppo
- invito di estranei alle lezioni in DDI

Procedure di segnalazione

Si rimanda agli allegati al cap.5 e, in ogni caso, si informa il Coordinatore di classe.

Azioni (gestione infrazione)

In misura proporzionale alla condotta segnalata, si metteranno in atto una o più delle seguenti misure, in base anche al Regolamento di Istituto:

- richiamo verbale
- ammonizione scritta sul registro elettronico
- convocazione genitori (Coordinatore di Classe)
- sanzione disciplinare (riunione straordinaria del CdC)
- azione educativa di sensibilizzazione sulla classe intera, in funzione dell'età (biennio/triennio)
- considerare la situazione personale dello studente (ad es. alunno con BES)
- intervento dello psicologo della scuola in classe
- supporto psicologico allo/la studente/ssa attraverso i servizi predisposti all'interno (Sportello d'ascolto) o all'esterno dell'istituto (necessita consenso del genitore se trattasi di minore)
- eventuale coinvolgimento della Polizia postale

I provvedimenti disciplinari ritenuti necessari saranno adottati dal Consiglio di classe in accordo con il Dirigente Scolastico.

Eventuali infrazioni nell'uso del device o della Rete compiute dal personale scolastico saranno gestite dal Dirigente Scolastico, secondo quanto previsto dal Codice di comportamento dei dipendenti pubblici (GU n.129 del 4-6-2013), dal CCNL (29 novembre 2007), dal DPCM (28 novembre 2000), dal Codice disciplinare e dalla normativa in vigore inerente alla privacy.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

Il documento di E-policy dialoga e si armonizza con gli altri regolamenti vigenti nell'Istituto, integrandosi pienamente con gli obiettivi enunciati nel PTOF, con il Regolamento di Istituto, con il Patto educativo di corresponsabilità controfirmato da Scuola, genitori e studenti all'atto dell'iscrizione, con il Piano scolastico per la didattica digitale integrata nel quale vengono individuati criteri e modalità di rimodulazione dell'attività didattica in regime di DDI.

Si indicano alcune proposte di modifica e/o integrazione dell'art.14 "Norme di comportamento" del Regolamento di Istituto, da definire e approvare nelle sedi opportune.

- Visto l'art. 3 del DPR 249/98 e successive modifiche di cui al DPR 235/2007 e la nota prot. 3602/PO del 31 Luglio 2008 (Statuto degli studenti e delle studentesse e successive modifiche);

- vista la Legge 547/93 (modificazioni e integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica);

- viste la Legge Regionale 24 Marzo 2016 e la Legge 71/2017 (normativa relativa ai fenomeni del bullismo e del cyberbullismo);

- visto il D.P.R. 390/90 e sue successive modifiche (T.U. delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazionedei relativi stati di tossicodipendenza);

- vista l'e-Policy d'Istituto;

Si individuano i comportamenti che si configurano come mancanze disciplinari:

- Integrazione del punto k dell'art.14: qualsiasi azione di hacking ai danni del registro elettronico e/o del sito della scuola (violazione e/o diffusione delle credenziali,alterazione, danneggiamento, cancellazione di dati o software…), anche ai fini della falsificazione.

- Integrazione del punto k dell'art.14: qualsiasi azione di hacking ai danni delle reti d'istituto (violazione e/o diffusione delle credenziali, alterazione, danneggiamento, uso delle reti per scopi o attività sanzionate dalla legge o comunque non previste dai Regolamenti specifici).

- Integrazione al punto k dell'art.14: di oggetti, di hardware, periferiche e software delle apparecchiature informatiche dell'Istituto.

- Integrazione del punto g dell'art.14: identità e orientamenti sessuali.

- Integrazione al termine del punto g dell'art.14: Rientrano in questa tipologia anche atti ascrivibili a sexting e pedopornografia.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'ePolicy 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 e l'eventuale aggiornamento del documento è a cura del Dirigente scolastico, coadiuvato dall'Animatore digitale, dal Referente per il bullismo e il cyberbullismo, dal Team per il contrasto al bullismo e al cyberbullismo, previa raccolta di feedback provenienti dalla comunità educante tutta.

Il Liceo "Bonghi Rosmini", in particolare, si impegna a valutarne l'incidenza e l'efficacia con cadenza annuale e ogni qual volta si dovessero verificare rilevanti variazioni in merito alla dotazione digitale della Scuola oppure si rendessero necessari adeguamenti alla normativa ministeriale sul tema.

L'efficacia del documento sarà testata con particolare riferimento agli obiettivi in esso esplicitati: promozione delle competenze digitali e dell'uso delle TIC nei percorsi educativi e didattici, prevenzione e gestione dei rischi connessi alla Rete, tutela del benessere socio-relazionale delle studentesse e degli studenti.

Il nostro piano d'azioni

Azioni da svolgere nei prossimi 3 anni:

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

Capitolo 2 - Formazione e 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, lavoraree 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.

Il curricolo sulle competenze digitali per gli studenti è trasversale alle discipline previste nel percorso di formazione scolastica. Il nostro Liceo sta elaborando un proprio curricolo, a partire dai documenti ministeriali di riferimento, nel quale tracciare i profili delle Competenze Chiave e di Cittadinanza e definire i curricoli verticali delle varie discipline per anno di corso. Nello specifico il curricolo delle competenze digitali si svilupperà secondo le 5 aree del quadro di riferimento DIGCOMP (Quadro comune di riferimento europeo per le competenze digitali):

1. ALFABETIZZAZIONE SU INFORMAZIONI E DATI: navigare, ricercare e filtrare dati, informazioni e contenuti digitali; valutare dati, informazioni e contenuti digitali; gestire dati, informazioni e contenuti digitali.

2. COMUNICAZIONE e COLLABORAZIONE: interagire attraverso le tecnologie digitali; condividere informazioni attraverso le tecnologie digitali; esercitare la cittadinanza attraverso le tecnologie digitali; collaborare attraverso le tecnologie digitali; gestire l'identità digitale.

2. CREAZIONE DI CONTENUTI DIGITALI: sviluppare contenuti digitali; integrare e rielaborare contenuti digitali; copyright e licenze; programmazione.

3. SICUREZZA: proteggere i dispositivi; proteggere i dati personali e la privacy: proteggere la salute e il benessere; proteggere l'ambiente.

4. RISOLVERE PROBLEMI: risolvere problemi tecnici; individuare fabbisogni e risposte tecnologiche; utilizzare in modo creativo le tecnologie digitali; individuare divari di competenze digitali. Per rendere fattiva l'acquisizione da parte degli studenti delle competenze digitali la scuola sta partecipando ad azioni previste dal PNSD e ai bandi promossi.

2.2 - Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

Il nostro Liceo ha promosso e realizzato iniziative di formazione dei docenti sull'utilizzo ed integrazione delle TIC nella didattica, anche se tale processo ha evidenziato rallentamenti a causa della situazione pandemica. In ottemperanza, poi, a quanto previsto dal programma del PNSD, molti docenti hanno partecipato ad attività di formazione realizzati all'interno degli snodi formativi territoriali o a corsi di formazione interna. Nella prospettiva del miglioramento dell'offerta formativa il percorso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica deve diventare, dunque, un processo permanente, in modo che le conoscenze siano il più possibile diffuse e condivise tra i docenti, sia attraverso momenti di autoformazione, che di formazione collettiva. Questo può avvenire incentivando la partecipazione dei docenti a tutte quelle iniziative di formazione su questi temi, promosse a livello ministeriale, a livello di scuole polo ed all'interno dell'istituzione scolastica.

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.

Il percorso della formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet prevede momenti di formazione, personale o collettiva, che devono tenere il passo alla veloce evoluzione sia delle tecnologie che delle modalità di comunicazione. Per realizzare tali interventi la scuola agirà su vari fronti:

1. organizzare corsi interni, sia predisposti dall'istituto che da scuole all'interno del polo formativo, per l'acquisizione di conoscenze e di approcci responsabili di fronte alle nuove tecnologie digitali, in considerazione del ruolo fondamentale che il docente assume in questo processo;

2. favorire la partecipazione a corsi esterni inerenti all'uso consapevole di Internet e delle tecnologie digitali che rispondano ad esigenze formative della scuola nel suo complesso.

3. informare i docenti su iniziative di formazione a distanza;

4. organizzare incontri con esperti esterni, in forma di seminari o dibattiti, che coinvolgano tutto il corpo docente.

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.

Per favorire la sinergia degli interventi educativi di scuola e famiglia e garantire il successo della prevenzione dei rischi connessi ad un uso non consapevole delle TIC è necessaria la collaborazione di tutti gli attori educandi, ognuno secondo i propri ruoli ele proprie responsabilità. Altrettanto importante è la promozione di un uso positivodelle TIC, capace di cogliere le opportunità offerte delle nuove Tecnologie. Per questa ragione il nostro Liceo 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. Pertanto, il presente documento è messo a disposizione di tutta la comunità scolastica e delle famiglie sul sito web d'Istituto assieme al Patto educativo di corresponsabilità stipulato con le famiglie. Tale documento costituisce l'impegno reciproco alla corresponsabilità formativa, nella quale rientrano pienamente i temi legati alla ePolicy. La scuola intende valorizzate le opportunità di incontro e formazione per le famiglie sui temi oggetto della Policy, selezionando iniziative significative promosse da Enti e/o Associazioni presenti sul territorio. Si promuoveranno momenti di confronto e discussione anche sulle dinamiche che potrebbero crearsi fra pari con l'uso di smartphone e social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dei treanni scolastici successivi)

- Organizzare e promuovere per il corpo docente incontri formativisull'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.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

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

Predisposizione e condivisione con l'intera comunità scolastica di un'informativa che illustri il ruolo del DPO, la tipologia di dati raccolti, il loro utilizzo e il fine per cui vengono utilizzati.

Predisposizione di apposito regolamento che disciplina l'uso di immagini e video. All'atto dell'iscrizione è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico di immagini e video. I nomi completi di alunne e alunni saranno evitati sul sito web come pure nei blog, forum e wiki, in particolare se in associazione con le loro fotografie.

Predisposizione di una liberatoria specifica per la condivisione di immagini e video durante eventi a carattere pubblico particolarmente rilevanti.

Predisposizione di una liberatoria specifica per la condivisione di elaborati ai fini della partecipazione a concorsi e a eventi pubblici.

Predisposizione di liberatorie specifiche, contenenti le modalità di trattamento, la conservazione dei dati raccolti e le misure di sicurezza adottate per la somministrazione di questionari di ricerca e per la partecipazione ad attività che coinvolgono personale esterno alla scuola.

Messa a disposizione dei genitori sul sito istituzionale del modello di reclamo al Garante per la protezione dei dati personali in caso di violazioni in materia di cyberbullismo.

Regolamentazione sull'uso di dispositivi in grado di registrare e di strumenti compensativi previsti nei PDP/PEI.

Inoltre:

1. Creazione sul sito di due "Aree riservate", una per i Docenti e una per il Consiglio di Istituto.

2. Definizione, sul sito istituzionale della scuola, di una specifica sezione dedicata Documento di ePolicy.

3. Pubblicazione, nella sezione Privacy, delle informative: agli studenti e alle loro famiglie al personale ai fornitori specifica per l'uso di G Suite (o altra piattaforma

similare) per la attività didattiche a distanza e documentali.

4. Pubblicazione, nella sezione Privacy, dei dati del DPO (nominativo, PEO, PEC, riferimento telefonico)

3.2 - Accesso ad Internet

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

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

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

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

Secondo il Piano Nazionale Scuola Digitale (PNSD), adottato con Decreto Ministeriale n. 851 del 27 ottobre 2015, la sfida dell'educazione nell'era digitale parte dall'accesso ad Internet. Il PNSD prevede interventi specifici, promossi e coordinati dall'Animatore Digitale, in merito alla formazione degli insegnanti, al miglioramento delle dotazioni hardware, fino alle attività didattiche. Per quanto riguarda la formazione l'animatore promuoverà la partecipazione a seminari, convegni, corsi on-line organizzati dagli Enti del territorio, dalle scuole in rete che partecipano al PNSD, da esperti interni e esterni alla Scuola. Tali interventi saranno rivolti ai docenti tutti e a quelli che avranno un profilo di accesso personale al sito, con il quale contribuiranno ad alimentare i contenuti didattici dello stesso; al personale amministrativo, dotato di un profilo di accesso personale al sito, che gestirà la comunicazione delle circolari, il registro elettronico e il personale; ai collaboratori scolastici, in primo piano nella comunicazione con gli utenti della scuola; alle famiglie, destinatarie di servizi on line. Il processo avverrà in modo graduale. Al fine di garantire la safety nell'accesso ad Internet gli studenti saranno guidati allo sviluppo di competenze digitali per un uso consapevole delle TIC e della RETE e al rispetto della "netiquette" (insieme di regole, comunemente accettate e seguite da quanti utilizzano Internet e i servizi di rete, che disciplinano il comportamento di un utente nel rapportarsi agli altri utenti attraverso risorse come wiki, newsgroup, mailing list, forum, blog o e-mail). L'Istituto si proponedi dotarsi di una PUA (Politica uso accettabile e sicurezza della rete): norme di buon utilizzo che la scuola si impegna a redigere e a divulgare prima che sia concesso l'accesso a Internet alla componente studentesca. La security sarà invece implementata attraverso l'adozione delle seguenti misure cautelative:

Mantenere separate le reti didattica e segreteria: importante per garantire maggiore sicurezza alle informazioni, gestendo in modo autonomo e con regole differenti le due reti grazie al firewall;

Aggiornare periodicamente software e Sistema operativo: garantire che il sistema sia aggiornato lo protegge dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo;

Definire la programmazione di backup periodici: cioè la copia e messa in sicurezza dei dati del sistema scolastico per prevenire la perdita degli stessi (possibilmente ancheuna copia offline);

Garantire formazione adeguata allo staff, incluso il corpo docenti: la formazione deve riguardare la gestione dei dispositivi, la conoscenza delle regole basilari sulla sicurezza;

Testare regolarmente le possibili vulnerabilità;

Preparare piani di azione in risposta ai problemi più seri: è importante non dover improvvisare nel momento in cui si verifica un problema serio, ma avere un protocollo di azione;

Predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di

inutilizzo: se non è previsto uno stand-by, il dispositivo resta accessibile nel caso in cui qualcuno dimentichi di spegnerlo, con il rischio potenziale di accesso da parte di persone non autorizzate;

Impostare il browser per l'eliminazione dei cookies alla chiusura: in questo modo si evita che qualcuno possa avere accesso ad account altrui senza autorizzazione;

Definire una policy sulle password;

Adottare il documento di ePolicy.

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 DS coordina la comunicazione interna ed esterna del nostro Istituto a partire da un piano di comunicazione in grado di trasmettere all'esterno l'identità, i valori, le azioni, i progetti e l'idea di educazione che la scuola porta avanti. Sono stati individuati i docenti responsabili del Sito Web e della pagina FB di Istituto. Sia la pagina Facebook che il sito web rispondono a specifici regolamenti approvati dal Consiglio di Istituto. Altri mezzi di comunicazione online in dotazione alla scuola sono: il registro elettronico con tutte le sue funzionalità, lo sportello di segreteria digitale e la sua bacheca istituzionale. Inoltre, attraverso l'account a dominio è possibile l'accesso in cloud a tutta una serie di applicazioni, tra cui Google Drive, Meet, Gmail, Chat e Hangouts che, nel loro insieme, costituiscono il sottosistema informatico per lacomunicazione e la collaborazione; la DDI, tramite Meet, Classroom, Calendar, Google Drive e gli altri applicativi della Suite di Google. Agli studenti e a tutto il personale della scuola è stato assegnato un account GSuite per il dominio dell'Istituto: nome.cognome@liceobonghi-rosmini.edu.it. Alle famiglie è stata inviata l'informativa riguardo all'uso e alle caratteristiche di Documento di e-policy, Per la messaggistica istantanea testuale o in videocall (docenti-docenti e docenti-genitori) si utilizzeranno Chat e Hangouts di Google Workspace, evitando di utilizzare WhatsApp, così come esplicitamente indicato dalle direttive europee. Sia per la DDI che per le riunioni in modalità telematica sono stati predisposti specifici regolamenti approvati dagli organi collegiali competenti. Il registro elettronico consente una comunicazione chiara e

immediata con le famiglie relativamente a:

1. andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari);

2. risultati scolastici (voti, documenti di valutazione);

3. udienze (prenotazioni colloqui individuali);

4. eventi (agenda eventi);

5. comunicazioni varie (comunicazioni di classe, comunicazioni personali).

Tutte le comunicazioni scuola-famiglia contenenti dati sensibili sono visibili da parte della famiglia dell'alunno interessato e non dal resto della classe. Solo il DS e i docenti del CdC possono avere accesso a tali informazioni. Il riepilogo delle medie con relative valutazioni ed eventuali assenze è accessibile sul registro elettronico AXIOS dal profilo dei Coordinatori di classe.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loroutilizzo 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.

Il Liceo Bonghi-Rosmini dispone il divieto dell'utilizzo del cellulare o di altri dispositivi elettronici per uso personale, se non autorizzato. La violazione di tale divieto configura un'infrazione disciplinare rispetto alla quale la scuola è tenuta ad applicare apposite sanzioni. Sia gli alunni (quando autorizzati dal docente) che i docenti sono tenuti a spegnere i propri cellulari prima dell'ingresso in aula. Per implementare la dotazione

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

Il nostro piano d'azioni

Il nostro piano d'azioni AZIONI:

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

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

Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.

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

Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity).

Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicurodelle tecnologie digitali (cybersecurity)

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

Premesso che, affinché la sensibilizzazione in relazione ad un determinato fenomeno possa essere efficace, è necessario che i destinatari del progetto siano consapevoli del problema e desiderino promuovere un cambiamento, il nostro Istituto si prefigge diprocedere in una duplice prospettiva:

Sensibilizzazione:

- incontri periodici per classi parallele, anche con soggetti esterni sui temi dei rischi online finalizzati ad accrescere la consapevolezza circa il problema;
- attività volte a incoraggiare il gruppo a modificare i propri comportamenti rendendoli più funzionali;
- incontri finalizzati a facilitare il coinvolgimento di soggetti esterni.

Prevenzione:

- progetti per promuovere le competenze digitali ed informare sui rischi connessi al loro uso e a quello della rete estesi non solo agli allievi, ma anche a genitori e docenti, con il coinvolgimento di figure professionali ed istituzionali (psicologi, polizia postale, etc.);
- azioni di contrasto al bullismo e al cyberbullismo.

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 siaquello 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 aggregazionegiovanile 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).

Si definiscono bullismo tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o a volte un piccolo gruppo). Si tratta, pertanto, di una serie di comportamenti ripetuti nel tempo. Quando queste vessazioni vengono consumate online, si parla di cyberbullismo.

Il cyberbullismo presenta le seguenti caratteristiche:

• è invasivo: il bullo può raggiungere la sua vittima in qualsiasi momento e in qualunque luogo;

• è un fenomeno persistente: il materiale messo online vi può rimanere per molto tempo;

• ha una platea potenzialmente infinita: le persone che possono assistere agli atti di cyberbullismo sono potenzialmente illimitate.

A seconda dei casi, si potranno adottare azioni di prevenzione universale, selettiva e indicata

1. Prevenzione Universale. Un programma di questo tipo parte dal presupposto che tutti gli studenti siano potenzialmente a rischio. Si tratta quindi di interventi diretti al grande pubblico o a un intero gruppo di una popolazione che non è stato identificatosulla base del rischio individuale. Efficacia: trattandosi di programmi ad ampio raggio gli effetti di questi programmi possono essere modesti se confrontati con programmi che "trattano" un gruppo con un problema specifico. Tuttavia, questi interventi possono produrre cambiamenti in grandi popolazioni.

2. Prevenzione Selettiva. Un programma dedicato ad un gruppo di studenti in cui il rischio online è presente. In questo caso la presenza del rischio è stata individuata tramite precedenti indagini, segnalazioni fatte dalla scuola, oppure dalla conoscenza della presenza di fattori di rischio in quel determinato territorio. In questi casi gli interventi sono mirati e prevedono programmi formativi strutturati che hanno l'obiettivo di migliorare le competenze digitali e le strategie di problem solving. Può essere un valido programma se si osservano casi in cui la prevenzione universale non ha dato gli esiti previsti.

3. Prevenzione Indicata. Un programma di intervento sul caso specifico è quindi pensato e strutturato per adattarsi agli/lle studenti/studentesse con l'obiettivo di ridurre i comportamenti problematici, oppure dare supporto alle vittime. Per la sua natura questo tipo di intervento si avvale di professionalità diverse perché spesso affronta problemi legati alla salute mentale del minore per cui è opportuno coinvolgere anche la famiglia del/lla ragazzo/a.

Il nostro Istituto, pertanto, ha nominato un referente che collaborerà con il Dirigente scolastico e si gioverà dell'apporto di docenti e figure di riferimento esterno al fine di stilare e/o integrare i regolamenti specifici.

Sarà poi avviata un'attenta attività di osservazione della popolazione studentesca, per valutarne bisogni e potenzialità.

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.

Per "hate speech" si intendono quelle pratiche che esprimono odio o intolleranza verso un gruppo o una persona identificata, ed avviene nella maggior parte dei

casi attraverso l'uso di internet. 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.

Inoltre, l'Istituto si potrà avvalere di consulenti/esperti esterni per organizzare incontri formativi rivolti a docenti, genitori ed alunni (Carabinieri, Polizia Postale, equipe Formazione Territoriale del MIUR, associazioni del Territorio preposte allo scopo...).

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?

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

L'Istituto si propone di promuovere un uso maggiormente consapevole delle tecnologie, per favorire il "benessere digitale", ossia la capacità di creare e mantenere una relazione sana con la tecnologia.

Pertanto il nostro Istituto si prefigge di:

- strutturare regole condivise e stipulare con gli allievi una sorta di "patto" d'aula, proponendo delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d'aula (adoperando, per esempio, la LIM o il dispositivo personale);
- dedicare al tema un momento specifico e riflettere con studenti e studentesse per fare in modo che la tecnologia sia strumento per raggiungere i propri obiettivi e non sia solo distrazione;
- creare una didattica per competenze trasversali, discutendo di cittadinanza digitale, di cyberbullismo, di uso integrativo e non sostitutivo dei dispositivi e della Rete.

Al fine di far maturare un approccio soddisfacente al digitale, si incentiverà la ricerca di equilibrio nell'uso degli strumenti digitali per il raggiungimento di obiettivi personali e la capacità di interagire negli ambienti digitali in modo sicuro e responsabile, nonché la capacità di gestire il sovraccarico informativo e le distrazioni

Se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi. È importante non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli studenti e delle studentesse, strutturando chiare e semplici regole condivise. Inoltre, sarà fondamentale concordare una linea condivisa con la famiglia, per stabilire mezzi e modalità durante lo studio domestico, con forme di controllo attivo durante la navigazione in Rete

4.5 - Sexting

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti 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.

"Spesso sono realizzate con il telefonino, e vengono diffuse attraverso il cellulare o attraverso siti, e-mail, chat. Spesso tali immagini o video, anche se inviate ad una

stretta cerchia di persone, si diffondono in modo incontrollabile e possono creare seri problemi, sia personali che legali, alla persona ritratta. L'invio di foto che ritraggono minorenni al di sotto dei 18 anni in pose sessualmente esplicite configura, infatti, ilreato di distribuzione di materiale pedopornografico".

I contenuti sessualmente espliciti, quindi, 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 612ter 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 eon 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.

Come riconoscerlo?

Per riconoscere un eventuale caso di adescamento online è importante prestare attenzione a piccoli segnali che possono essere indicatori importanti, come ad esempio un cambiamento improvviso nel comportamento di un minore. A seguire, alcuni segnalie domande che potrebbero esserci di aiuto:

- Il minore ha conoscenze sessuali non adeguate alla sua età?
- Venite a conoscenza di un certo video o di una foto che circola online o che il minore ha ricevuto o filmato, ma c'è imbarazzo e preoccupazione nel raccontarvi di più...
- Il minore si isola totalmente e sembra preso solo da una relazione online?
- Ci sono prese in giro e allusioni sessuali verso un bambino/ragazzo in particolare?

L'importanza di un'adeguata educazione all'affettività e alla sessualità

Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e

non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e perché no, della sessualità.

Nella società digitale, attraverso la Rete, i minori definiscono se stessi, si raccontano e sperimentano nuove forme di identità, socializzano, si emozionano e si relazionano con gli altri, scoprono la propria sessualità e giocano con essa.

Tutto ciò risponde a bisogni assolutamente naturali e importanti, ma allo stesso tempo può esporre i ragazzi a possibili rischi come quello, appena approfondito, dell'adescamento online.

Il desiderio di conferma sociale (da ottenere anche attraverso i social) e, talvolta, lascarsa consapevolezza degli adolescenti nel gestire la propria immagine online quando pubblicano sui loro profili social video e foto piuttosto intimi o sensuali, può aumentare il rischio di esporli ad un adescamento online. Con un'adeguata competenza digitale ed emotiva, Internet potrebbe essere un valido supporto per i/le ragazzi/e nel loro percorso di esplorazione della sessualità. Purtroppo, però, non è sempre così. La Rete, infatti, abbonda di contenuti inadeguati che offrono una rappresentazione distorta della sessualità e dei rapporti uomo-donna. La sessualità in Rete è spesso rappresentata in modo decontestualizzato e senza alcun richiamo alla dimensione affettiva ed emotiva dei soggetti. Il più delle volte, tali rappresentazioni ricalcano con forza stereotipi di genere come quello della "donna oggetto" e quello dell' "uomo fortee virile", tanto più forte e virile quanto più è in grado di conquistare e dominare quell'"oggetto".

In un contesto simile non c'è da stupirsi se, talvolta, anche i comportamenti degli adolescenti in Rete nella gestione della propria sessualità o semplicemente della propria immagine online riproducano tali modelli. Modelli che la società odierna sembra tuttora confermare in numerosi messaggi che quotidianamente ci arrivano attraverso i media.

La problematica dell'adescamento online (come quella del sexting), quindi, si inquadra in uno scenario più ampio di scarsa educazione emotiva, sessuale e di assenza di competenza digitale, in riferimento al modo in cui i/le ragazzi/e vivono la propria sessualità e la propria immagine online, al loro desiderio di esprimersi e affermare se stessi.

Fondamentale quindi, come sappiamo, è portare avanti un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è).

Come intervenire?

Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere, ad esempio, all'adescatore. È importante che il computer o altri dispositivi elettronici della minore vittima non vengano usati per non compromettere eventuali prove.

Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video…).

L'adescamento, inoltre, può essere una problematica molto delicata da gestire e puòavere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.

I minori vittime di adescamento riferiscono, generalmente, di sentirsi traditi, ma anche di provare un senso di colpa per essere caduti in trappola ed essersi fidati di uno sconosciuto.

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

Per consigli e per un supporto è possibile rivolgersi alla Helpline di Generazioni Connesse (19696): operatori esperti e preparati sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che dei bambini, degli adolescenti, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti l'utilizzo dei nuovi media.

4.7 - Pedopornografia

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

La legge n. 269 del 3 agosto 1998 *"Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come, ad esempio, il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella* ***legge n.***

38 del 6 febbraio 2006 *"Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet"*, segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.)che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

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

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

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

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

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

Se nella nostra scuola si ravvisasse un rischio per il benessere psicofisico dei/lle bambini/e, ragazzi/e coinvolte nella visione di contenuti pedopornografici, si renderà opportuno ricorrere alle autorità competenti (Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Polizia di Stato – Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza), provvedendo contestualmente a fornire un supporto psicologico anche passando per una consultazione presso il medico di base o pediatra di riferimento.

In tale contesto 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.

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 delle hotline.

Il nostro piano d'azioni

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

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

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

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

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

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

- **Cyberbullismo**: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalitàattraverso 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.

Sono da considerare degni di segnalazione:

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

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

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

---

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 preparazionee 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.

Il Liceo Bonghi-Rosmini ha individuato i docenti del Team Anti Bullismo e Cyberbullismo che faranno da supporto agli altri docenti nella formazione e il monitoraggio degli eventuali casi e i docenti del Team per l'Emergenza che valuteranno in maniera approfondita le segnalazioni e sceglieranno la strategia di intervento più opportuna.

In relazione al **CASO A**, è opportuno che i docenti coinvolgano il Referente d'Istituto per il contrasto del bullismo e del cyberbullismo, al fine di valutare le possibili strategie d'intervento. Se si ravvisano gli estremi, viene informato il Dirigente scolastico unitamente al Consiglio di classe. Uno strumento utile per raccogliere informazioni può essere il diario di bordo (allegato alla presente ePolicy). Operativamente è fondamentale coinvolgere tutti gli studenti e le studentesse, informandoli sui fenomeni e sulle caratteristiche degli stessi, suggerendo di chiedere aiuto se pensano di vivere situazioni, di subire atti identificabili come bullismo o cyberbullismo.

In relazione al **CASO B**, il docente deve condividere immediatamente quanto osservato con il Referente per il bullismo e il cyberbullismo, attraverso il MODULO DI PRIMA SEGNALAZIONE che deve essere compilato e consegnato all'indirizzo mail fgpc15000c@istruzione.it all'attenzione del referente bullismo. La prima segnalazione può essere effettuata da qualsiasi docente, dai genitori/tutori e, nella secondaria, dagli stessi studenti e ha lo scopo tenere una traccia della presa in carico della situazione e delle prime informazioni sull'accaduto.

Il Referente attiva il team per l'emergenza che, dopo una valutazione approfondita,

determinerà le strategie di intervento di più idonee. Se non si ravvisano fattispecie di reato, è opportuno:

informare i genitori (o chi esercita la responsabilità genitoriale) degli/delle studenti/studentesse direttamente coinvolti/e (qualsiasi ruolo abbiano avuto), se possibile con la presenza di professionisti dell'aiuto, per strategie condivise e modalità di supporto;

creare momenti di confronto costruttivo in classe, con la presenza di figure specialistiche territoriali;

informare i genitori degli/delle studenti/studentesse infra-quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy);

informare gli/le studenti/studentesse ultraquattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o Social (o successivamente, in caso di non risposta, al garante della Privacy);

convocare il consiglio di classe;

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

A seconda della situazione e delle valutazioni effettuate con Referente, Dirigente e genitori, si potrebbe poi segnalare alla Polizia Postale -ove necessario ai sensi di legge:

a. contenuto del materiale online offensivo;

b. modalità di diffusione;

c. fattispecie di reato eventuale.

Se è opportuno, richiedere un sostegno ai servizi e alle associazioni territoriali o ad altre autorità competenti. E' bene sempre dialogare con la classe, attraverso interventi educativi specifici, cercando di sensibilizzare studenti e studentesse sulla necessità di non diffondere ulteriormente online i materiali dannosi, ma anzi di segnalarli e bloccarli.

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 casidi 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.

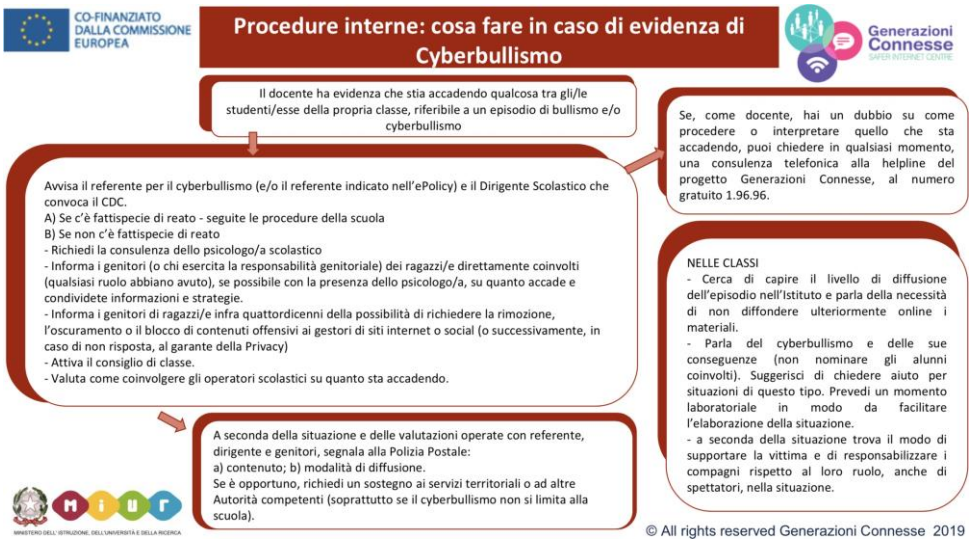
Al fine di prevenire episodi di bullismo/cyberbullismo e diffondere consapevolezza su questi temi, il Liceo Bonghi-Rosmini organizza incontri con esperti ed eventi formali rivolti a tutti gli Studenti/Studentesse, Docenti e Genitori, come, ad esempio, iniziative

legate alla Giornata contro il bullismo e cyberbullismo, o moduli di Educazione Civica e progetti PCTO.

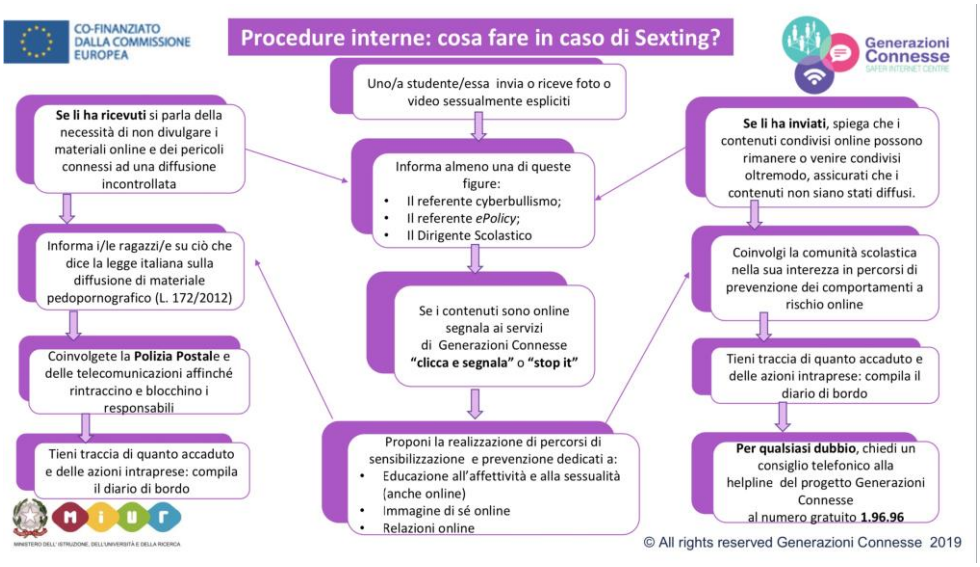
Presso il Liceo Bonghi-Rosmini è comunque presente uno sportello di psicologia-psicoterapia attivato annualmente con lo scopo di incrementare il benessere psicofisico degli allievi.

5.4. - Allegati con le procedure

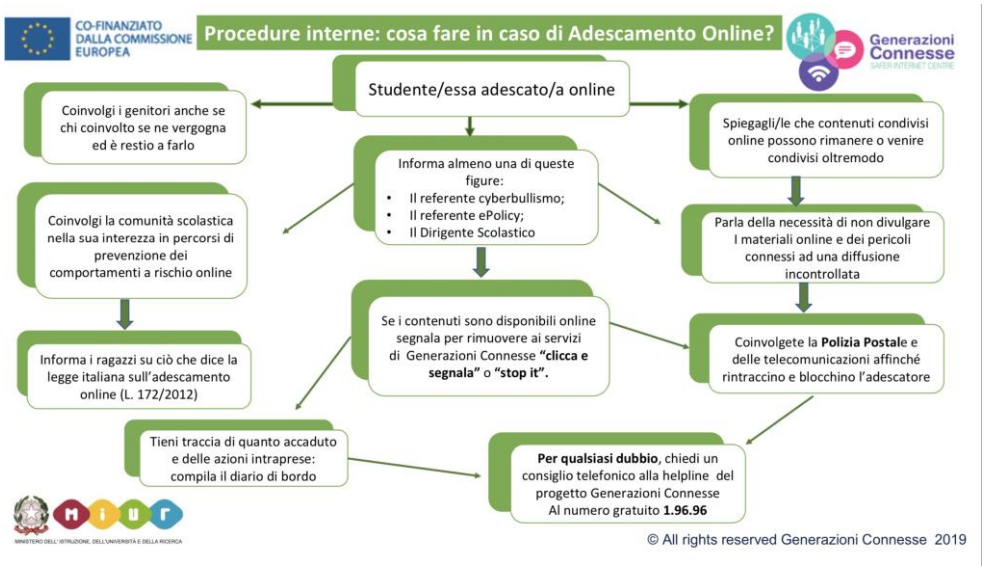
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



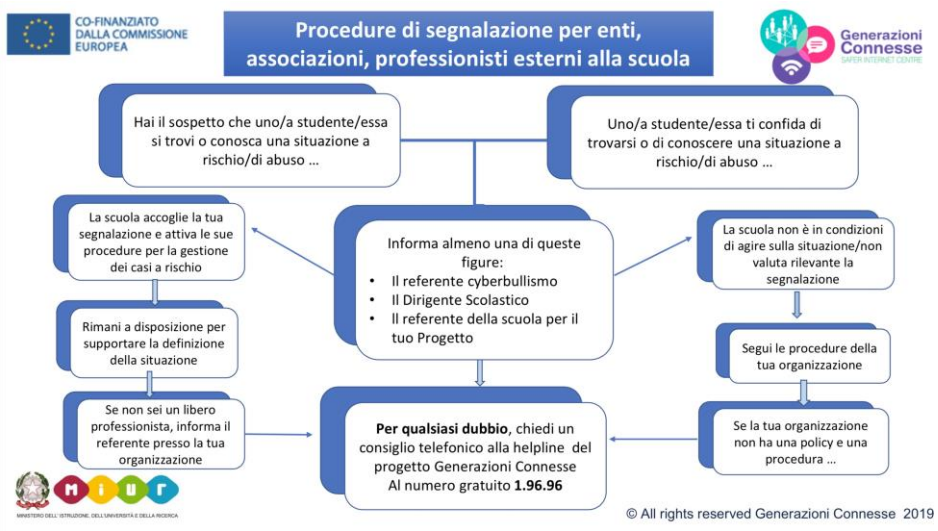
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Il Liceo Bonghi-Rosmini ha fatto proprie ed adottato specifiche procedure previa formazione ePolicy ed ELISA dei Docenti. La modulistica per la segnalazione (Modulo di prima segnalazione) e gestione (Modulo di valutazione approfondita) dei casi sono pubblicati sulla pagina dedicata del sito web di istituto. Per la gestione dei casi di emergenza si fa riferimento al Protocollo di intervento approvato dal Collegio dei Docenti.

Il nostro piano d'azioni

Sulla base delle Linee Guida per l'uso positivo delle tecnologie digitali e della prevenzione dei rischi nelle scuole, vengono assunti i seguenti puntiper una collaborazione sinergica tra scuola-famiglia-servizi territoriali, al fine di creare un modello composito e lineare di azioni condivise:

- coinvolgimento di tutti gli attori della scuola: studenti e studentesse, docenti, genitori e personale ATA, per la realizzazione di una autentica comunità educante;

- alleanza educativa tra scuola e famiglia;

- interventi educativi ed azioni di supporto, quale prevenzione per eventuali comportamenti a rischio;

- misure preventive specifiche di tutela anche con l'ausilio di attori territoriali, come Polizia postale;

- promozione dell'educazione al rispetto;

- sviluppo del pensiero critico;

- promozione dell'Educazione Civica Digitale.