Documento di ePolicy

LEPS01000P

LICEO SCIENTIFICO"DE GIORGI"LECCE

V.LE M. DE PIETRO 14 - 73100 - LECCE - LECCE (LE)

Giovanna Caretto

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

1.2 - Ruoli e responsabilità

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

Il Dirigente Scolastico

- promuove e garantisce la formazione e l'aggiornamento del personale docente e non docente sulla sicurezza e sulla prevenzione di problematiche offline e 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;

- offre il proprio contributo all'organizzazione, insieme al docente referente, sulle tematiche del bullismo/cyberbullismo, favorendo iniziative di formazione e prevenzione del fenomeno;
- implementa corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC;
- ha la responsabilità di intervenire nei casi più gravi di bullismo, cyberbullismo e uso improprio delle tecnologie digitali;
- stimola l'attenzione di genitori e alunni alle problematiche connesse alla sicurezza in rete.

L'Animatore Digitale e il team digitale

- supportano la comunità scolastica sugli aspetti tecnico informatici, sui rischi online e sulla protezione e gestione dei dati personali
- promuovono percorsi di formazione interna per la scuola al fine di garantire l’acquisizione e lo sviluppo delle competenze digitali (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell’ambito dell’educazione civica);
- promuovono l'adesione ai bandi relativi allo sviluppo delle competenze digitali e si impegnano nelle relative attività di progettazione e di realizzazione;
- rilevano e gestiscono le problematiche connesse all'utilizzo delle TIC;
- controllano che gli utenti autorizzati accedano alla rete della scuola con apposita password, per scopi istituzionali e consentiti;
- favoriscono la dematerializzazione delle attività relative alla didattica e l'informatizzazione delle comunicazioni scuola-famiglia
- interagiscono e cooperano 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 delle forze di Polizia, dello psicologo operante nella scuola, 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 nella propria didattica 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 tecnologici;
- sensibilizzano gli studenti all'uso consapevole delle risorse fornite dalla rete;
- segnalano, in quanto Pubblici Ufficiali, al Dirigente Scolastico eventuali problematiche o casi di violenza e abuso on-line in cui siano coinvolti gli studenti, nel momento in cui ne vengano a conoscenza.

Il personale ATA

- garantisce supporto tecnico a studenti e docenti nei laboratori che prevedono l'uso della LIM e di altri dispositivi
- è coinvolto nelle attività di formazione e di autoformazione in tema di bullismo e cyberbullismo e uso responsabile della rete.
- 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

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 e presenti nel PTOF e nei vari regolamenti di Istituto;
- imparano a tutelare sé stessi e i propri compagni dai rischi on-line;
- 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, comunicando

- tempestivamente al dirigente e/o ai docenti, eventuali usi poco responsabili della rete da parte dei propri figli;

- leggono, accettano e condividono, all'atto dell'iscrizione, la E-policy dell'Istituto.

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).

I soggetti esterni che sono responsabili di iniziative educative e formative nell'Istituto

- prendono visione del documento ePolicy dell'Istituto riguardo l'uso consapevole e responsabile della rete e delle TIC;
- promuovono la sicurezza on-line durante le attività di cui sono titolari;
- segnalano ai docenti preposti e al Dirigente Scolastico eventuali comportamenti problematici o casi di abuso nell'uso della rete e delle TIC.

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

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

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

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

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

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

da compilare con le indicazioni contenute nella lezione

1.5 - Gestione delle infrazioni alla ePolicy

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

da compilare con le indicazioni contenute nella lezione

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.

da compilare con le indicazioni contenute nella lezione

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

da compilare con le indicazioni contenute nella lezione

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Creazione del gruppo di lavoro E-policy, così costituito: referente per la prevenzione del bullismo e del cyberbullismo, FS PTOF, Animatore digitale, FS Sostegno allo Studente;
- Organizzazione di una riunione in avvio di anno scolastico dei Coordinatori di Dipartimento per discutere delle attività relative all'E-policy.

Azioni da svolgere nei prossimi tre anni:

- Realizzazione di un sistema di rilevazione e monitoraggio delle attività di prevenzione e formazione (somministrazione a campione di questionari nelle classi sulle azioni di prevenzione del bullismo e del cyberbullismo)
- Monitoraggio sull'efficacia dell'E-policy attraverso sondaggio rivolto a tutte le componenti dell'Istituto
- Formazione del personale docente e non docente sui reati on-line e sulla privacy;
- Revisione/aggiornamento del Regolamento d'Istituto
- Implementazione della dotazione tecnica sia per le classi sia per docenti e studenti (comodato d’uso), con particolare attenzione nei confronti degli allievi con BES, nei limiti delle dotazioni finanziarie dell'Istituto e dei fondi dedicati.

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

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

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

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

Aree di competenza

- informazione
- comunicazione
- creazione di contenuti
- problem-solving

- sicurezza

Descrittori di competenza

Lo studente:

- identifica, localizza, recupera, conserva le informazioni digitali secondo un approccio "intuitivo";
- identifica, localizza, recupera le informazioni digitali con consapevolezza e con atteggiamento critico;
- conserva, organizza e analizza le informazioni digitali;
- comunica in ambienti digitali, condivide risorse attraverso strumenti on-line, sa collegarsi con gli altri e collabora attraverso strumenti digitali;
- interagisce e partecipa alle comunità e alle reti;
- realizza e modifica contenuti (da elaborazione testi a immagini e video);
- integra e rielabora conoscenze, produce contenuti in modo creativo;
- utilizza gli strumenti digitali per identificare e risolvere piccoli problemi tecnici;
- contribuisce alla creazione di conoscenza, produce risultati creativi ed innovativi, supporta gli altri nell'uso degli strumenti digitali;
- riflette e acquisisce consapevolezza su protezione personale, protezione dei dati, protezione dell’identità digitale, misure di sicurezza;
- conosce ed applica i diritti di proprietà intellettuale e le licenze.

Strumenti

- Rete e connettività;
- registro elettronico e ambiente di lavoro condiviso: Moodle e Google Suite (Gmail, Google Drive, Google Hangouts, Google Calendar e Google Documenti,

…) come ambiente informatico ad accesso gratuito per la gestione e condivisione di materiale didattico (corsi, verifiche formative e sommative, prove comuni, Video didattici in rete - es. YouTube, OVO, risorse digitali dei manuali in adozione, RAI Scuola, RAI Play -;

- Software per la produzione di documenti, fogli di calcolo e presentazioni
- Software di geometria dinamica (es. Geogebra, Desmos, Tinkercad)
- Software per la didattica collaborativa (es. Padlet, Google Maps, EdModo, Weschool, Etwinning, Pik-to-chart, Storyboard that, Speak-Pic)
- Software per lo sviluppo del pensiero computazionale e il making educativo (es. Cura, pacchetto Autodesk)
- Software per la realizzazione di mappe concettuali (es. CMap) e video tutorial (es. Premiere, Windows media player, Powtoon)
- Software per videoconferenza (Zoom, Skype, …)

Traguardi formativi

- Utilizzare la rete per scopi di informazione, comunicazione, ricerca e svago
- Utilizzare strumenti informatici e di comunicazione per elaborare dati, testi e immagini e produrre documenti
- Conoscere le caratteristiche e le potenzialità tecnologiche degli strumenti d'uso più comuni (PC, tablet, smartphone, strumenti archiviazione memoria digitale)
- Riconoscere vantaggi, potenzialità, limiti e rischi connessi all'uso delle tecnologie più comuni, anche informatiche
- Apprendere a utilizzare gli "aggregatori" digitali
- Cogliere e sfruttare le potenzialità creative e non solo quelle funzionali delle applicazioni digitali
- Apprendere a discriminare le fonti di informazione più affidabili

Presso il Liceo De Giorgi sono stati inseriti moduli di Educazione alla cittadinanza digitale, relativi al diritto alla connessione, come diritto fondamentale dell'uomo, al rispetto e ai limiti della libertà di espressione on-line. Tali tematiche vengono trattate con riferimento alla normativa vigente, al dibattito giuridico internazionale, alla storia dei diritti umani. In molti percorsi didattici, predisposti nelle programmazioni curriculari, viene, inoltre, favorita e implementata l'individuazione di "aggregatori" digitali, cioè software complessi, piattaforme o semplici applicazioni, che favoriscono un lavoro sistematico su criteri e processi di aggregazione e gerarchizzazione delle informazioni. Gradualmente, viene insegnata agli studenti l'importanza della creazione - e non solo della fruizione - di contenuti digitali.

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 Liceo 'C. De Giorgi', ha favorito, nel corso degli ultimi dieci anni, l'inserimento delle tecnologie informatiche nella didattica (registro elettronico, LIM, ambienti di condivisione) sia nella prospettiva dell'inclusione in relazione ai Bisogni Educativi Specifici, sia, più in generale, per adeguare, anche nella forma della comunicazione didattica, un percorso di apprendimento in grado di promuovere il successo formativo di tutti e di ciascuno, con metodologie didattiche innovative. L'utilizzo e l'integrazione delle Tic nella didattica sono avvenuti nel rispetto della libertà di insegnamento e delle propensioni personali del singolo docente.

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.

Infatti presso il Liceo De Giorgi è stata incentivata la formazione dei docenti sulle tematiche dell'inclusione, dell'uso consapevole delle TIC (uso della Lim, uso del Registro Elettronico, piattaforma Moodle, Suite di Google, programmi e applicazioni per la creazione di mappe). Il Liceo De Giorgi prevede l'attivazione di corsi e incontri sui rischi on line, sul bullismo e sul cyberbullismo.

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.

Tra le attività di sensibilizzazione, coinvolgimento e collaborazione delle famiglie si

intende procedere a una rilevazione rivolta alla componente genitori per individuare i temi che necessitano di maggiore approfondimento nell'ambito dell'educazione alla cittadinanza digitale e dell'inclusione.

Il Patto di Corresponsabilità, contiene già le seguenti integrazioni:

- garantire il rispetto della privacy di studenti e famiglie secondo quanto previsto dalla Privacy policy pubblicata sul sito dell'Istituto;
- far rispettare le norme di comportamento previste dal Regolamento di Istituto e dalla E-policy di Istituto;
- far osservare le norme di sicurezza e prevenzione, anche in relazione all'uso appropriato delle tecnologie informatiche e di comunicazione;
- sottoporre agli Enti Esterni, coinvolti in attività di progetto e/o di PCTO dell'Istituto, in sede o in ambienti esterni, la E-policy d'Istituto;
- comunicare agli Enti Esterni, coinvolti in attività di progetto e/o di PCTO dell'Istituto, in sede o in ambienti esterni, le procedure di segnalazione di eventuali abusi o reati on-line che vedano come vittime o autori gli studenti.

Il nostro piano d'azioni

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

- prevenzione bullismo e cyberbullismo nelle classi prime e seconde
- promozione di percorsi formativi per lo sviluppo delle competenze digitali
- avvio della fase istruttoria per la redazione della E-policy

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

- inserimento nel PTOF (2022-2025) del documento di e-policy;

- coinvolgimento delle famiglie per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale;
- organizzazione e promozione di incontri formativi per il corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali;
- organizzazione di incontri con esperti sulle competenze digitali, sull'educazione alla cittadinanza digitale

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

In relazione al nuovo Regolamento Generale sulla Protezione dei Dati, (UE) 679/2016 "GDPR" con effetti diretti a partire dal 25 maggio 2018, recepito in Italia col decreto legislativo n.101 del 10-08-2018, vigente dal 19 settembre 2018, che inserisce la figura obbligatoria nella P.A. del Responsabile della Protezione dei Dati (RPD), per agevolare l'applicazione del GDPR.

3.2 - Accesso ad Internet

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

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

reti pubbliche di comunicazioni mobili all'interno dell'Unione".

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

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

L'istituto gode di una strumentazione tecnologica diffusa capillarmente in tutti gli spazi, grazie ai finanziamenti europei statali PON, a quelli della Regione, ai progetti del Piano Nazionale Scuola Digitale, nonché al contributo volontario delle famiglie (canone per la connettività e ristrutturazione dei laboratori multimediali. La connettività è garantita dalla fibra ottica in modalità via cavo e Wi-Fi ed offre la connessione ad Internet per le attività sia didattiche sia amministrative.

La rete della segreteria è separata dalla rete didattica e, grazie ad un diverso firewall e ad un server dedicato, gestisce in modo in modo autonomo e con regole differenti la sicurezza. Il Dirigente Scolastico, il Direttore dei Servizi Generali e Amministrativi ed il personale degli uffici della segreteria sono profilati con account personalizzati e accedono ai servizi tramite procedura di autenticazione personale che prevede l'utilizzo di password aventi caratteristiche adeguate.

L'assistenza tecnica del server e delle apparecchiature informatiche è affidata ad una ditta specializzata nel settore, che provvede al controllo sul backup dei dati, all'aggiornamento dei sistemi operativi e degli antivirus installati sulle macchine e al controllo del funzionamento del firewall.

La rete didattica, dotata di firewall dedicato, fornisce in sicurezza la connessione alle classi provviste di strumentazione tecnologica, ai laboratori scientifici, multimediali, alla biblioteca e alle aule multifunzionali destinate al lavoro dei docenti. Il firewall non permette l'accesso ai siti non attendibili e ai social.

In tutti questi spazi l'utilizzo quotidiano del registro elettronico è gestito da Spaggiari che ne garantisce la protezione dei dati, così come la normativa richiede. L'accesso alla strumentazione e alla connessione è consentito ai docenti solo ai fini didattici ed è normato da password gestite dal responsabile della rete Lan-Wlan dell'Istituto e dagli assistenti tecnici informatici. Gli studenti accedono alla rete sotto il controllo dei docenti durante le attività didattiche.

La sensibilizzazione rispetto all'uso delle password viene fatta attraverso la diffusione di circolari circa l'utilizzo della strumentazione tecnologica da parte dei docenti.

In particolare gli assistenti tecnici informatici hanno cura di aggiornare periodicamente il software e il sistema operativo a garanzia della protezione da aggressioni esterne e dalle vulnerabilità che emergono nel tempo.

L'uso della tecnologia a scuola riguarda tutta l'attività didattica (sia in presenza che a distanza) per cui sia i docenti sia gli studenti adottano le indicazioni previste dai regolamenti approvati dal Consiglio di Istituto circa l'accesso alla Rete e ai dispositivi tecnologici. I regolamenti sono pubblicati sul sito web della scuola.

3.3 - Strumenti di comunicazione online

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

Gli strumenti che l'Istituto adotta sono: Sito scolastico, Registro Elettronico, Mail personali e/o istituzionali.

Sito scolastico

L'animatore digitale cura la redazione editoriale e la gestione delle pagine del sito del liceodegiorgi.edu.it; il Dirigente Scolastico è garante del contenuto.

La scuola detiene i diritti d'autore dei documenti che si trovano sul proprio sito o di quei documenti per i quali è stato chiesto ed ottenuto il permesso dall'autore proprietario. Le informazioni pubblicate sul sito della scuola relative alle persone da contattare rispettano le norme vigenti sulla privacy.

La scuola non pubblica sul proprio sito materiale prodotto dagli alunni senza il permesso dei loro genitori; inoltre, le fotografie degli stessi sono pubblicate previa liberatoria dei genitori o tutori.

Per la tutela, sicurezza e protezione dei dati trattati, il Liceo ricorre a

- utilizzo del protocollo HTTPS (l'Hypertext Transfer Protocol Secure è un protocollo per la comunicazione su Internet che protegge l'integrità e la riservatezza dei dati scambiati on line);

- utilizzo di un sistema di cifratura quando il trattamento di dati lo richiede (ovvero oscurare il dato per renderlo incomprensibile a coloro che non hanno i codici per accedervi, mediante la "crittografia" e, quindi, l'uso di un algoritmo di cifratura);

- sistema di backup (sistema che permette di salvare regolarmente i dati, di ripristinare eventuali file modificati o rimossi per errore dalla rete, di garantire la presenza di una copia di sicurezza di tutti i file importanti).

La scuola offre all'interno del proprio sito web i seguenti servizi alle famiglie ed agli utenti esterni:

- servizio del Registro on-line per comunicazione di voti e assenze e per prenotazione di colloqui individuali con i docenti

- segreteria digitale (pubblicazione delle circolari della Presidenza)

- consultazione elenchi libri di testo

- Piano triennale dell'Offerta Formativa

- Regolamento di Istituto

- Patto di Corresponsabilità

- Orario delle lezioni.

Registro elettronico - Piattaforma Spaggiari

Docenti

- Ad ogni docente è assegnato un accesso con password per la gestione del registro elettronico e posta elettronica dell'Istituto.

- Ogni docente firma la presenza secondo l'orario scolastico e tiene aggiornato il registro personale. Ogni docente chiude il Registro Elettronico al termine della

lezione.

- Ogni docente chiude su ogni postazione la casella di posta utilizzata sia quella personale sia quella messa a disposizione dell'Istituto.

- L'Istituto non risponde dell'alterazione di eventuali dati.

Famiglie

- I genitori e gli alunni maggiorenni accedono al Registro Elettronico con un profilo assegnato dal sistema, per la comunicazione sull'andamento didattico-disciplinare dell'alunno, per la prenotazione dei colloqui mattutini e pomeridiani e per prendere atto della programmazione didattica.

Dirigente, Collaboratori, Segreteria

- La comunicazione formale con le famiglie avviene tramite l'invio dalla mail istituzionale della scuola alle mail personali dei genitori.

3.4 - Strumentazione personale

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

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

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

Strumentazione personale

Per gli studenti

Durante le attività didattiche gli studenti sono autorizzati ad utilizzare la strumentazione personale quali cellulari, tablet ecc. solo ed esclusivamente per uso didattico e sotto il controllo del docente; altresì agli allievi non è permesso utilizzare i telefoni cellulari per telefonare, scattare foto, registrare filmati durante le lezioni o durante l'orario scolastico. È vietato inviare messaggi illeciti o inappropriati, nonché fotografie o filmati. La connessione ai servizi di internet per la propria strumentazione viene fatta su rete personale.

Agli alunni con BES o DSA la scuola garantisce il supporto tecnologico idoneo e l'uso della strumentazione personale con l'accesso alla rete wifi dell'istituto.

Per i docenti

Durante le ore delle lezioni non è consentito l'utilizzo del cellulare se non per finalità strettamente didattica. È consentito l'uso di altri dispositivi elettronici personali sempre solo a scopo didattico ed integrativo di quelli scolastici disponibili. Durante il restante orario di servizio è permesso l'uso di portatili, tablet, per attività funzionali all'insegnamento in entrambe le situazioni ed è garantito l'accesso alla rete wifi negli spazi comuni previsti dalla logistica della rete stessa.

Per il personale della scuola

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

Il nostro piano d'azioni

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

- Formazione del personale docente e non docente dell'Istituto, degli studenti e delle studentesse, sul tema delle tecnologie digitali e della

protezione dei dati personali.

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

Almeno 1 di queste 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 incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Attività di monitoraggio

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.*

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

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

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

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
    - Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
    - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d’istituto), atti e documenti (PTOF, PdM, Rav).

Le azioni previste dal PTOF 2019-2022 in relazione a questa problematica:

- partecipazione ad eventi e incontri della Polizia Postale

- cicli di incontri con la Polizia di Stato, per le classi del biennio per la prevenzione del bullismo e del cyberbullismo; con l'Arma dei Carabinieri per le classi quinte per la prevenzione e la sensibilizzazione sui reati legati all'utilizzo di internet e delle piattaforme on-line

- presenza a scuola di referente bullismo e cyberbullismo

- attivazione dello Sportello d'ascolto, in presenza e servizio di consulenza on-line

---

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.

- partecipazione ad eventi e incontri della Polizia Postale

- cicli di incontri con la Polizia di Stato, per le classi del biennio per la prevenzione del bullismo e del cyberbullismo; con l'Arma dei Carabinieri per le classi quinte per la prevenzione e la sensibilizzazione sui reati legati all'utilizzo di internet e delle piattaforme on-line

- presenza a scuola di referente bullismo e cyberbullismo

- attivazione dello Sportello d'ascolto, in presenza e servizio di consulenza on-line.

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?

Le azioni che il nostro Istituto che intende intraprendere in relazione a questa problematica sono:.

- partecipazione ad eventi e incontri della Polizia Postale
- cicli di incontri con la Polizia di Stato, per le classi del biennio per la prevenzione del bullismo e del cyberbullismo; con l'Arma dei Carabinieri per le classi quinte per la prevenzione e la sensibilizzazione sui reati legati all'utilizzo di internet e delle piattaforme on-line
- presenza a scuola di referente bullismo e cyberbullismo
- attivazione dello Sportello d'ascolto, in presenza e servizio di consulenza on-line

---

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.

Le azioni che il nostro Istituto che intende intraprendere in relazione a questa problematica sono:.

- partecipazione ad eventi e incontri della Polizia Postale
- cicli di incontri con la Polizia di Stato, per le classi del biennio per la prevenzione del bullismo e del cyberbullismo; con l'Arma dei Carabinieri per le classi quinte per la prevenzione e la sensibilizzazione sui reati legati all'utilizzo di internet e delle piattaforme on-line
- presenza a scuola di referente bullismo e cyberbullismo
- attivazione dello Sportello d'ascolto, in presenza e servizio di consulenza on-line

---

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.

- partecipazione ad eventi e incontri della Polizia Postale
- cicli di incontri con la Polizia di Stato, per le classi del biennio per la prevenzione del bullismo e del cyberbullismo; con l'Arma dei Carabinieri per le classi quinte per la prevenzione e la sensibilizzazione sui reati legati all'utilizzo di internet e delle piattaforme on-line
- presenza a scuola di referente bullismo e cyberbullismo
- attivazione dello Sportello d'ascolto, in presenza e servizio di consulenza on-line

---

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.

Le azioni che il nostro Istituto che intende intraprendere in relazione a questa problematica sono:

- partecipazione ad eventi e incontri della Polizia Postale
- cicli di incontri con la Polizia di Stato, per le classi del biennio per la prevenzione del bullismo e del cyberbullismo; con l'Arma dei Carabinieri per le classi quinte per la prevenzione e la sensibilizzazione sui reati legati all'utilizzo di internet e delle piattaforme on-line
- presenza a scuola di referente bullismo e cyberbullismo
- attivazione dello Sportello d'ascolto, in presenza e servizio di consulenza on-line

Il nostro piano d'azioni

AZIONI (sviluppate nell'arco dell'anno scolastico 2019/2020).

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

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

Almeno due di queste azioni

- Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti
- Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli/delle studenti/studentesse
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/delle studenti/studentesse
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/alle studenti/studentesse.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

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

segnalare la presenza di materiale pedopornografico online.

5.2. - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

- CASO A (SOSPETTO) – Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.
- CASO B (EVIDENZA) – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

Per tutti i dettagli fate riferimento agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto

Generazioni Connesse, al numero gratuito 1.96.96.

In presenza di sospetto relativo a un episodio di cyberbullismo, basato su testimonianza diretta o diretta visione di prodotti informatici di tipo denigratorio o usati a tal fine (foto, post, video, ...), il docente, venuto a conoscenza dei fatti nell'esercizio delle proprie funzioni, in qualità di Pubblico Ufficiale (art. 357 c.p. e art. 331 c.p.p.), relaziona al Dirigente Scolastico per iscritto, avendo cura di far protocollare la propria segnalazione, da inoltrarsi preferibilmente a mano in busta chiusa. Il Dirigente deve comunicare per iscritto al docente l'avvenuta trasmissione all'autorità competente. Qualora ciò non avvenisse entro i due giorni lavorativi successivi al protocollo, il docente stesso dovrà inoltrare la segnalazione. In particolare, nei casi di reati perseguibili d'ufficio (per es. sexting, pedopornografia, adescamento on-line, ...) o in caso si sospetti grave pregiudizio per il minore, il docente, informato dei fatti, in qualità di Pubblico Ufficiale, denuncia immediatamente all'autorità di P.S. o all'autorità giudiziaria, dandone comunicazione al Dirigente Scolastico. In caso sia individuata la vittima, il Dirigente Scolastico o, su delega, il Vicario e/o il Secondo Collaboratore, e/o il coordinatore di classe, e/o il referente per il bullismo o cyberbullismo, deve convocare i genitori (o chi esercita la responsabilità genitoriale) e informarli dei fatti, eventualmente con il supporto degli esperti dello sportello di ascolto.

La convocazione dei genitori non deve essere fatta per i reati di sexting, pedopornografia o per altri reati in cui sia possibile che la vulnerabilità del minore nasca all'interno del nucleo familiare. Gli studenti, che vivano in prima persona o come testimoni situazioni problematiche, possono rivolgersi ai docenti di classe, al coordinatore di classe, al Dirigente Scolastico, al referente per il contrasto del bullismo e del cyberbullismo, alla psicologa operante all'interno dell'Istituto, a qualsiasi commissariato di P.S., al commissariato on-line (https://www.commissariatodips.it/), alla Polizia Postale, all'Arma dei Carabinieri. Inoltre, gli studenti possono inviare la propria segnalazione, anche in forma anonima, tramite l'applicazione YouPol della Polizia di Stato (https://www.poliziadistato.it/statics/40/presentazione_youpol_-esserci.pdf.pdf).

In particolare, i minori che ritengano che determinanti contenuti a loro riferiti e diffusi per via telematica (foto e/o video imbarazzanti e/o offensivi, pagine web e/o post sui social network in cui si è vittime di minacce e/o offese e/o insulti, ecc.) siano atti di cyberbullismo, ne possono richiedere l'oscuramento, la rimozione o il blocco. Le richieste vanno inviate al titolare del trattamento o al gestore del sito o del social media dove sono pubblicati i contenuti ritenuti atti di cyberbullismo. L'istanza può essere inoltrata direttamente dal minore, se ha più di 14 anni, oppure da chi esercita la responsabilità genitoriale. Nel caso la richiesta non venga soddisfatta, ci si può rivolgere al Garante per la protezione dei dati personali, che, entro 48 ore, provvede in

merito alla segnalazione (legge n 71/2017). Per inoltrare le segnalazioni si può utilizzare il modello disponibile su www.garanteprivacy.it/cyberbullismo, inviandolo via e-mail a cyberbullismo@gpdp.it. Gli psicologi operanti all'interno dell'Istituto scolastico, gli addetti del personale ATA, gli esperti esterni coinvolti in attività di docenza per attività dell'Istituto (progetti, PCTO, corsi ...), in sede o fuori sede, ricoprono il ruolo di Operatori Incaricati di Pubblico Servizio (art.358 c.p.) e come tali sono obbligati a denunciare e o segnalare i fatti appartenenti alle tipologie sopradescritte, di cui sono informati per testimonianza diretta o visione diretta di materiale che rientri nelle categorie di reati precedentemente indicati. Pertanto, sono tenuti a mettere in atto le procedure contenute nei precedenti paragrafi, comunicando, inoltre, per iscritto, al docente con cui abitualmente hanno contatti (referente di progetto, coordinatore di classe, docente della classe), i fatti di cui sono venuti a conoscenza e l'avvenuta segnalazione al Dirigente Scolastico e/o all'autorità di P.S. e/o all'autorità giudiziaria. Il consiglio di classe a cui appartenga lo studente o il gruppo di studenti coinvolto nei fatti, previa informativa da parte del titolare della segnalazione/denuncia o da parte del Dirigente Scolastico, attiva percorsi di informazione, prevenzione e sensibilizzazione, avvalendosi, se giudicato opportuno, del supporto di esperti esterni quali psicologi, servizi sociali, forze dell'ordine, Polizia Postale, ecc. E' fondamentale che venga rispettato il segreto d'ufficio sull'identità dei soggetti implicati, indipendentemente dal loro ruolo. Il consiglio di classe e, a seconda della gravità della violazione, il Consiglio d'Istituto valutano l'eventuale erogazione di provvedimenti o sanzioni disciplinari nelle sedi, nelle modalità e con le finalità previste dal Regolamento d'Istituto e dallo Statuto degli Studenti e delle Studentesse.

In tutte queste procedure, gli studenti, le famiglie, il personale ATA, gli esperti esterni, i docenti e il Dirigente Scolastico possono avvalersi della figura del referente per il contrasto al bullismo e al cyberbullismo.

5.3. - Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

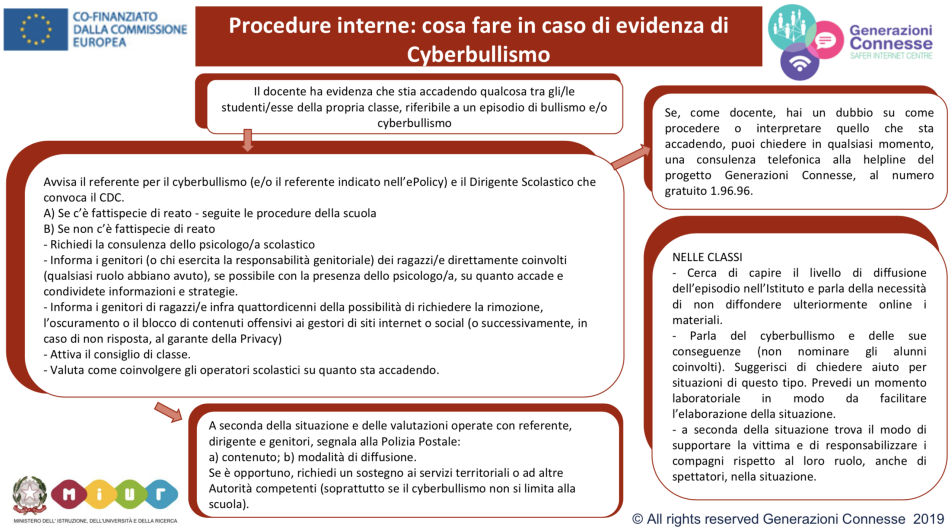
Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

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

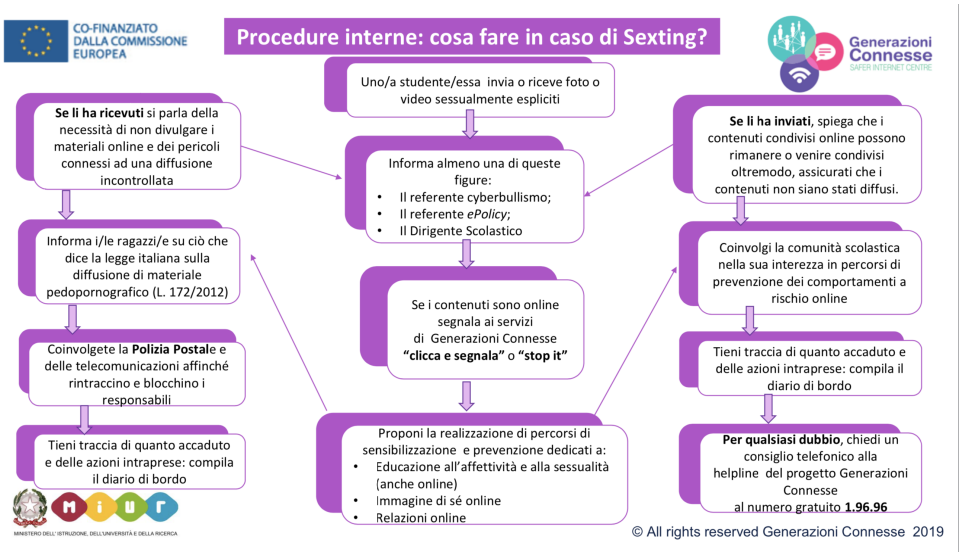
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni**: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico**: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

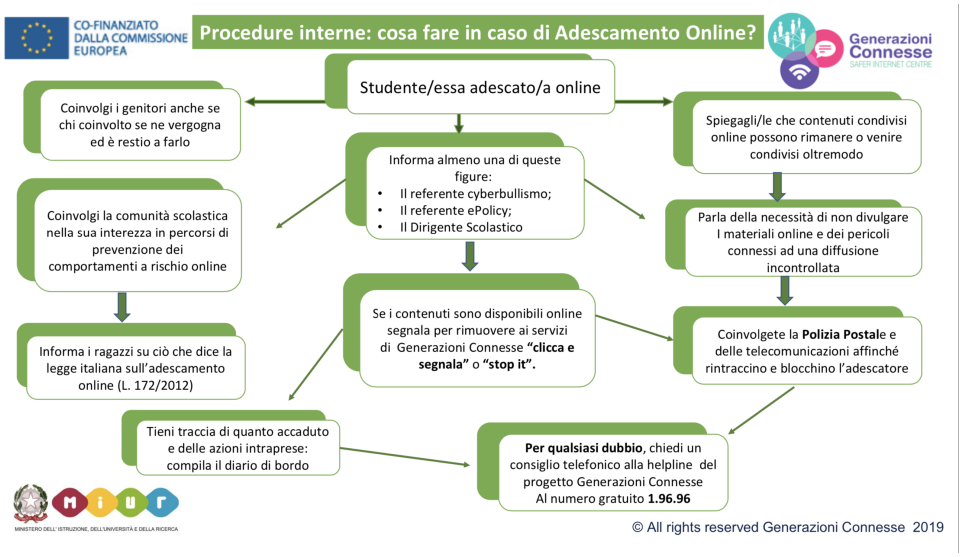
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



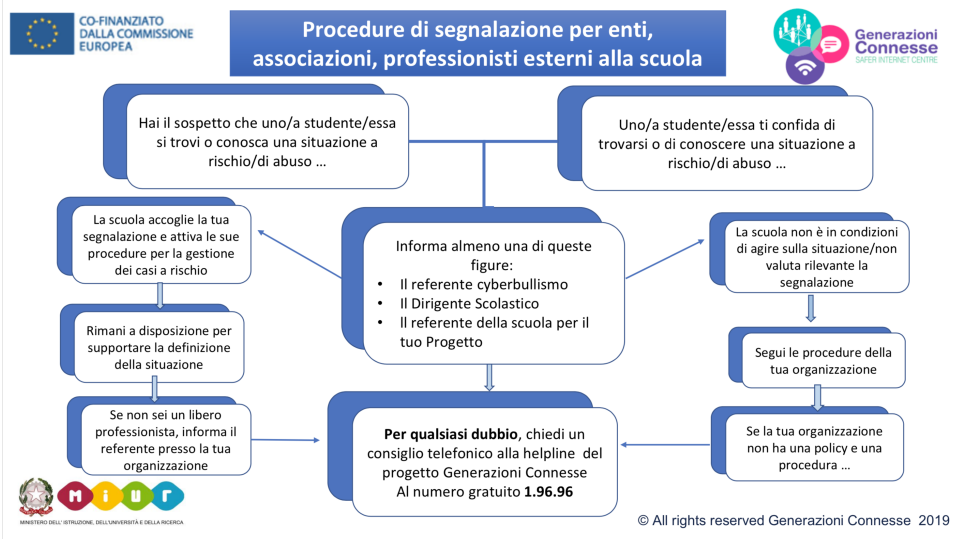
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Il nostro piano d'azioni

Non è prevista nessuna azione.