Documento di ePolicy

FGIC88200L

Istituto Comprensivo "Via Pietro Nenni"

VIA PIETRO NENNI 13/15 - 71017 - TORREMAGGIORE - FOGGIA (FG)

Dirigente Scolastico prof. Matteo Scarlato

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.

Lo scopo dell' ePolicy è di condividere e stabilire con tutti i membri della comunità scolastica regole, modalità e principi sull’utilizzo consapevole e corretto di internet.
La scuola opererà ,eventualmente, in stretto collegamento con le forze dell'ordine e con le istituzioni del settore educativo, per mettere in campo strategie di prevenzione al cyberbullismo e interventi di recupero nel caso in cui vengano individuati tali fenomeni, informando i genitori/tutori e chiedendo la loro collaborazione. Le indicazioni, contenute nella presente e-Safety Policy, intendono dare al nostro Istituto un impulso allo sviluppo all'uso corretto e consapevole di Internet e di tutte le finestre connesse al digitale.

I principi fondamentali richiamati sono:

1) Proteggere i bambini, i ragazzi e tutto il personale dell'Istituto;

2) assistere il personale della scuola a lavorare in modo sicuro e responsabile con le tecnologie di comunicazione di Internet;

3) impostare dei comportamenti di condotta adeguati e regolamentati in base alla normativa vigente;

4) garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che il comportamento illecito è inaccettabile e che saranno intraprese le opportune azioni disciplinari e/o giudiziarie. Gli utenti, siano essi maggiorenni o minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete.

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.

Di seguito si elencano ruoli e responsabilità del nostro Istituto:

Il Dirigente Scolastico

il Dirigente Scolastico garantisce la sicurezza, anche online, di tutti i membri della

comunità scolastica. In linea con il quadro normativo di riferimento e le indicazioni del MIUR, promuove la cultura della sicurezza online e, ove possibile, dà il proprio contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC. Inoltre, il Dirigente Scolastico è responsabile di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

L'Animatore digitale

L'Animatore digitale supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali, oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica); inoltre, rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola, e ha il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti.

Il Referente bullismo e cyberbullismo

Tale figura ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio. Fondamentale è, dunque, il suo ruolo non solo in ambito scolastico ma anche in quello extrascolastico, in quanto potrebbe coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.

I Docenti

i Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Innanzitutto, integrano parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo anche l'uso delle tecnologie digitali nella didattica. I docenti accompagnano e supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete; hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

Il personale Amministrativo, Tecnico e Ausiliario

Il personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il dirigente scolastico e con il personale docente tutto. Diverse figure che, in sinergia, si occupano ciascuno per la propria funzione, del funzionamento dell'Istituto scolastico che passa anche attraverso lo sviluppo della cultura digitale e dell'organizzazione del tempo scuola. Il personale ATA, all'interno dei singoli regolamenti d'Istituto, è coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo, insieme ad altre figure e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo.

Gli Studenti e le Studentesse

Gli Studenti e le Studentesse devono, in relazione al proprio grado di maturità e consapevolezza raggiunta, utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola imparano a tutelarsi online; a tutelare i/le propri/e compagni/e e rispettarli/le; a partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e a farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education.

I Genitori

i Genitori, in continuità con l'Istituto scolastico, devono partecipare alle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali; devono relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet.

Gli Enti educativi esterni e le associazioni

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola devono conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC; devono, inoltre, promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme. Dato il quadro normativo, rispetto ad un profilo prettamente processuale anche in materia di bullismo e cyberbullismo, si può parlare di tre tipologie di "culpa":

- culpa in vigilando: concerne la mancata sorveglianza attiva da parte del docente responsabile verso il minore (cosi come da art. 2048 del c.c.). Tale condizione è superabile se ci si avvale di una prova liberatoria di non aver

potuto impedire il fatto (recita il terzo comma dell'art. 2048 c.c.: "le persone indicate nei commi precedenti sono liberate dalla responsabilità soltanto se provano di non aver potuto impedire il fatto").

- culpa in organizzando: si riferisce ai provvedimenti previsti e presi dal Dirigente Scolastico ritenuti come non soddisfacenti e quindi elemento favorevole al verificarsi dell'eventuale incidente.
- culpa in educando: fa capo ai genitori i quali hanno instaurato una relazione educativa con il/la figlio/a, ritenuta come non adeguata, insufficiente o comunque carente tale da metterlo/a nella situazione di poter recare danno a terzi.

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).

L'Istituto si impegna a diffondere il presente documento per condividerne i contenuti con tutta la comunità scolastica. Il documento sarà comunicato al personale, agli alunni e alla comunità scolastica nel seguente modo:

- Pubblicazione della E-Safety Policy sul sito della scuola.

Pertanto, tutti i soggetti esterni dovranno rispettare il regolamento della Policy dell'

Istituto.

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.

Come citato nella sezione precedente, il documento verrà comunicato attraverso i canali ufficiali scolastici. E' utile specificare le varie modalità di condivisione con i vari attori e studenti dell'Istituto. Tale condivisione avverrà secondo le seguenti modalità:

1) Condivisione e comunicazione del documento agli alunni attraverso:

- la discussione in classe della policy, con particolare riguardo al protocollo di utilizzo di internet per tutte le classi;

- la formazione degli alunni riguardo all'uso responsabile e sicuro di internet;

- l' educazione sulla sicurezza agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili.

Inoltre, tra le misure di prevenzione che la scuola metterà in atto, ci saranno azioni finalizzate a promuovere una cultura dell'inclusione e del rispetto dell'altro con l'utilizzo delle strumentazioni digitali.

2) Condivisione e comunicazione del documento al personale attraverso:

- La comunicazione sui canali ufficiali.

- la formazione sulla piattaforma www.generazioniconnesse.it.

Il sistema di monitoraggio sarà supervisionato dall'Animatore digitale che segnalerà al DS o al DSGA eventuali problemi che dovessero richiedere acquisti o interventi tecnici.

3) Condivisione e comunicazione del documento ai genitori attraverso:

- Il sito web della scuola;

- un approccio di collaborazione ;

- l'informazione sui siti d'interesse;

- informazione sui corsi d'aggiornamento da svolgere sulla piattaforma e-Policy sul sito www.generazioniconnesse.it.

Si richiede ad ogni genitore e/o tutore l'impegno a far rispettare ai propri figli il documento anche in ambito domestico, vigilando sull'utilizzo della rete da parte dei minori.

1.5 - Gestione delle infrazioni alla ePolicy

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

Le infrazioni del documento possono essere rilevate da tutto il personale nell'esercizio delle proprie funzioni. Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. La scuola prenderà tutte le precauzioni necessarie per garantire la sicurezza on-line. Nel caso in cui le infrazioni della policy violino norme previste dal Regolamento di Istituto si procede secondo quanto previsto dallo stesso; qualora le infrazioni riguardino l'opportunità di certi comportamenti o la convivenza civile, la scuola eroga delle sanzioni secondo il principio della sensibilizzazione e del risarcimento dell'eventuale danno provocato, in uno spirito di recupero e rieducazione.

I provvedimenti includono:

- Possibile allontanamento dall' utilizzo dei device concordato con i genitori;

- possibilità di non far utilizzare il cellulare per alcuni giorni. (Da concordare con il genitore) ;

- le denunce di bullismo online saranno trattate in conformità con la legge attuale;

- nei casi più gravi, saranno avviate le comunicazioni alle autorità competenti.

E' bene ricordare a tutti che nel momento in cui un qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia.

1) Disciplina degli alunni

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali e internet, in relazione alla fascia di età considerate, sono prevedibilmente le seguenti:

- Un uso della rete per giudicare, infastidire o impedire, in modo persistente , a qualcuno di esprimersi o partecipare ;

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

- la condivisione impropria di link delle classi dell'Istituto utilizzati per la DaD;

-eventuale invio o condivisione di immagini intime o personali;

- il collegamento a siti web, nell'orario scolastico, non autorizzati dai docenti.

2) Disciplina del personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet sono diverse:

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

- un utilizzo delle comunicazioni non compatibili con il ruolo professionale;

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

- non aver formato gli alunni a un uso consapevole degli strumenti digitali.

3) Disciplina dei genitori

Generalmente le situazioni familiari meno favorevoli sono:

- Una posizione del computer in una stanza non visibile a tutti quando è utilizzato dal proprio figlio;

- piena autonomia concessa al proprio figlio nella navigazione sul web senza condivisione o controllo della cronologia;

- la mancanza di adeguata conoscenza che la responsabilità dei contenuti non idonei utilizzati dai minori è sempre ascrivibile ai genitori o tutori ;

- assoluto disinteresse per i propri figli.

CAPITOLO INTEGRATIVO (COVID-19)

Didattica digitale Integrata

Gli alunni vengono informati del fatto che l'utilizzo di Internet è monitorato e vengono date loro istruzioni per un uso responsabile e sicuro.Tutto il personale scolastico, pertanto, è coinvolto nel monitoraggio dell'utilizzo di Internet, nello sviluppo delle linee guida e nell'applicazione delle istruzioni sull'uso sicuro e responsabile di Internet. Il monitoraggio dell'implementazione della policy e del suo eventuale aggiornamento sarà svolta ogni anno. Tale monitoraggio sarà curato dal Dirigente scolastico con la collaborazione dell'Animatore digitale , dal referente del cyber bullismo e dai docenti delle classi. Vista la situazione pandemica, il nostro Istituto, ha creato un regolamento specifico per il comportamento corretto durante la didattica digitale integrata (DDI).
Di seguito, un estratto dal Piano Scolastico sulle buone pratiche, da parte degli alunni, sull'utilizzo della DDI:

Modalità di svolgimento delle attività sincrone

Durante lo svolgimento delle video-lezioni agli alunni è richiesto il rispetto di quanto previsto nell'addendum al Regolamento di Istituto e, in particolare delle seguenti regole:

· Accedere alla lezione con puntualità, secondo quanto stabilito dall'orario settimanale delle video-lezioni o dall'insegnante. Il link di accesso alla lezione è strettamente riservato, pertanto è fatto divieto a ciascuno di condividerlo con soggetti esterni alla classe o all'Istituto;

· accedere alla lezione sempre con microfono disattivato. L'eventuale attivazione del microfono è richiesta dall'insegnante o consentita dall'insegnante su richiesta della studentessa o dello studente.

· in caso di ingresso in ritardo, non interrompere l'attività in corso;

· partecipare ordinatamente alla lezione. Le richieste di parola sono rivolte all'insegnante sulla chat o utilizzando gli strumenti di prenotazione disponibili sulla piattaforma;

· partecipare alla lezione con la videocamera attivata che inquadra l'alunno stesso in primo piano, in un ambiente adatto all'apprendimento e possibilmente privo di rumori

di fondo, con un abbigliamento adeguato e provvisti del materiale necessario per lo svolgimento dell'attività. La partecipazione alla lezione con la videocamera disattivata è consentita solo in casi particolari e su richiesta motivata dell'alunno all'insegnante prima dell'inizio della sessione. Dopo un primo richiamo, l'insegnante attribuisce una nota disciplinare alle studentesse e agli studenti con la videocamera disattivata senza permesso, li esclude dalla video lezione e l'assenza dovrà essere giustificata.

Responsabilità

Gli alunni:

· Hanno il dovere di seguire le indicazioni dettate regolarmente dai docenti al fine di non interrompere il processo formativo avviato.

· Si impegnano a partecipare in maniera seria e responsabile alle attività di DDI.

· Si impegnano a inviare, nelle modalità indicate dai docenti, i compiti e le attività assegnate, comunicando tempestivamente eventuali difficoltà, per consentire ai docenti di individuare soluzioni alternative.

· Partecipano alle video-lezioni in diretta, assumendo comportamenti adeguati e rispettosi di tutti.

· Sono responsabili delle attività che si effettuano tramite l'account personale e si impegnano ad adoperarsi per salvaguardare la riservatezza delle proprie credenziali di accesso e a segnalarne l'eventuale smarrimento.

· Al termine delle attività didattiche, e nel caso in cui lo stesso dispositivo digitale sia usato da più persone, dovrà uscire dall'account istituzionale (logout) onde evitare che per errore egli stesso, o altri componenti della famiglia, possano accedere ad altri social, forum o piattaforme con l'account dell'istituto. In caso di momentaneo allontanamento dalla postazione, effettuare il logout dalle piattaforme e spegnere la postazione di lavoro e/o utilizzare altri strumenti tecnici (screen saver con password) per impedire la visualizzazione di documenti con dati personali salvati sul dispositivo.

· Non registreranno e non condivideranno, per alcun motivo, le video-lezioni in diretta.

· Assumeranno, all'interno delle chat, un comportamento corretto e rispettoso di tutti. · Contatteranno prontamente i docenti per segnalare difficoltà tecniche e/o didattiche per consentire alla Scuola di intervenire per risolverle.

· Segnaleranno eventuali episodi inadeguati o scorretti, di cui vengano direttamente o indirettamente a conoscenza, relativi all'uso degli strumenti attivati per la didattica a distanza.

· Si atterranno a quanto previsto dallo Statuto delle studentesse e degli studenti e nel Patto di Corresponsabilità per l'a.s.2020/21.

· Durante le video-lezioni indosseranno un abbigliamento consono all'attività didattica,

dando ad esse la stessa valenza delle lezioni in presenza, cercando di posizionarsi in un ambiente il più possibile “neutro” (evitando di riprendere es. foto, poster, altri componenti del nucleo familiare, specie se minori, ecc.). Divieti

· La piattaforme sono e saranno attivate per uso esclusivamente educativo-didattico: per questo motivo, è vietato utilizzare l’account della scuola per attività o scopi di tipo privato che non hanno a che fare con la scuola stessa.

· Per operare all’interno delle piattaforme (visionare gli inviti alle lezioni, interagire con la piattaforma ecc.) si deve essere in possesso e conseguentemente accedere con l’account istituzionale.

· È fatto assoluto divieto di divulgare i link alle lezioni ad utenti terzi esterni alla scuola, se non previa autorizzazione dell’organizzatore.

· È assolutamente vietato diffondere foto o stralci delle video-lezioni. È vietata, pertanto, la pubblicazione su altri siti o canali Social anche dell’Istituto non dedicati alla formazione a distanza con gestione degli accessi e suddivisione delle risorse per classi.

· È severamente vietato offendere qualsiasi partecipante durante le video-lezioni: tutte le regole di correttezza e rispetto dell’altro valgono nella modalità online come nella modalità in presenza. · È severamente vietato violare la privacy degli utenti o inviare materiale non didattico. Se si aggiunge materiale, assicurarsi di non eliminare altri elaborati prodotti dagli utenti. Non diffondere eventuali informazioni riservate di cui si viene a conoscenza, relative ad altri utenti; non pubblicare contenuti protetti dalla tutela del diritto d'autore e materiali non attinenti alle attività didattiche.

· Non è consentito invitare utenti non presenti nella organizzazione istituzionale (che non abbiano l’account istituzionale). I menzionati comportamenti sono non solo vietati ma anche perseguibili giuridicamente, in quanto contrari alla normativa civile e penale vigente, pertanto, ove si riscontrassero o venissero segnalate anomalie e/o comportamenti illeciti si prenderanno provvedimenti disciplinari nei confronti dei responsabili, e se necessario, si adirà per vie legali per concorso o favoreggiamento nei seguenti reati perseguibili per legge: - Violazione della privacy

- Interruzione di pubblico servizio - Furto di identità - Accesso abusivo ai sistemi informatici. A tal proposito si ricorda che tutte le video-lezioni realizzate sono monitorate da consolle di amministrazione e tutti i movimenti in entrata e in uscita, nonché le chat dei partecipanti alle riunioni, sono registrate e tracciate.

Per quanto concerne i docenti e/o genitori restano in vigore le indicazioni presenti nei punti precedenti.

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.

Con l'approvazione della Policy, sarà possibile delineare un percorso unilaterale sull'organizzazione dell'utilizzo dei dispositivi digitali. In tal senso, sarà possibile allineare il materiale presente in questo documento con le indicazioni del Patto di Corresponsabilità, in coerenza con le Linee Guida del Miur e tutta la normativa sui temi in oggetto.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il documento ePolicy sarà riesaminato quando si verificheranno cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola e tutte le modifiche della Policy saranno discusse in dettaglio con i componenti del gruppo ePolicy. Nell'ambito del monitoraggio si terranno in considerazione i dati annuali raccolti dal gruppo specifico con la collaborazione del gruppo docenti.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni

Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori

Azioni da svolgere nei prossimi 3 anni:

- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- 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, 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.

Il gruppo di lavoro partirà dal curricolo di scuola già improntato per progettare un percorso più dettagliato.

Il curricolo sulle competenze digitali farà riferimento alle seguenti fonti legislative:

- Raccomandazione del Parlamento Europeo 2006 (che richiamano alle diverse dimensioni delle competenze digitali: dimensione tecnologica e dimensione cognitiva).
- Piano Scuola Digitale (PNSD).
- Raccomandazione del Consiglio dell'Unione Europea 2018.
- Sillabo sull'Educazione Civica Digitale.
- DigComp 2.1.: "Il quadro di riferimento per le competenze digitali dei cittadini", con otto livelli di padronanza.
- Raccomandazione del Consiglio europeo relativa alle competenze chiave per

l'apprendimento permanente.

Il DigComp prevede:
aree di competenze individuate come facenti parte delle competenze digitali;
descrittori delle competenze e titoli pertinenti a ciascuna area (21 competenze);
livelli di padronanza per ciascuna competenza (i livelli sono 8);
conoscenze, abilità e attitudini applicabili a ciascuna competenza.

Le aree di competenza individuate dal Digcomp sono, nello specifico: **Area 1**: "Alfabetizzazione e dati": capacità di cercare, selezionare, valutare e riprocessare le informazioni in Rete.

- Navigare, ricercare e filtrare dati, informazioni e contenuti digitali;
- valutare e gestire dati, informazioni e contenuti digitali;
- saper riconoscere e sapersi difendere da contenuti dannosi e pericolosi in Rete.

Area 2: "Comunicazione e collaborazione" :modalità appropriate per comunicare e relazionarsi online.

- Saper interagire con gli altri attraverso le tecnologie digitali;
- essere consapevoli nella condivisione delle informazioni in Rete;
- essere buoni "cittadini digitali";
- collaborare adeguatamente con gli altri attraverso le tecnologie digitali;
- conoscere le "Netiquette", ovvero le norme di comportamento online;
- saper gestire la propria "identità digitale".

Area 3: "Creazione di contenuti digitali"
Quest'area fa riferimento alle capacità di "valutare le modalità più appropriate per modificare, affinare, migliorare e integrare nuovi contenuti e informazioni specifici per crearne di nuovi e originali".

- Creare e modificare contenuti digitali in diversi formati per esprimersi attraverso mezzi digitali;
- modificare, affinare, migliorare e integrare informazioni e contenuti all'interno di un corpus di conoscenze esistente per creare conoscenze e contenuti nuovi, originali e rilevanti;
- capire come il copyright e le licenze si applicano ai dati, alle informazioni e ai contenuti digitali.

Area 4: "Sicurezza"
Quest'area è parte di una dimensione più generale definita come "benessere digitale" che include la necessità di salvaguardare i propri dati personali e rispettare le regole nel trattare i dati altrui.

- Imparare a proteggere i dispositivi e i contenuti digitali e comprendere i rischi e le minacce presenti negli ambienti digitali. Conoscere le misure di sicurezza e protezione e tenere in debita considerazione l'affidabilità e la privacy;

- proteggere i dati personali e la privacy negli ambienti digitali. Capire come utilizzare e condividere informazioni personali proteggendo se stessi e gli altri dai danni. Comprendere che i servizi digitali hanno un "regolamento sulla privacy" per informare gli utenti sull'utilizzo dei dati personali raccolti;
- conoscere (ed esercitare) i propri diritti in termini di privacy e sicurezza.

Il documento dovrà definire descrittori e livelli di padronanza più dettagliati rispetto al curricolo in essere e prevedere rubriche valutative.

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.

Così come previsto nel PNSD, attraverso le TIC, sono promosse iniziative di formazione dei docenti, anche mediante l'organizzazione di laboratori formativi (senza necessariamente un formatore), favorendo l'animazione e la partecipazione di tutta la comunità scolastica alle attività formative, come ad esempio quelle organizzate attraverso gli snodi formativi.

I docenti favoriscono la partecipazione e stimolano il protagonismo degli studenti nell'organizzazione di workshop e altre attività, anche strutturate, sui temi del PNSD, attraverso momenti formativi aperti alle famiglie e ad altri attori del territorio, per la realizzazione di una cultura digitale condivisa.

Individuano soluzioni metodologiche e tecnologiche sostenibili da diffondere all'interno degli ambienti della scuola (es. uso di particolari strumenti per la didattica di cui la scuola si è dotata; la pratica di una metodologia comune; informazione su innovazioni esistenti in altre scuole; un laboratorio di coding per tutti gli studenti), coerenti con l'analisi dei fabbisogni della scuola stessa, anche in sinergia con attività di assistenza tecnica condotta da altre figure.

Il piano triennale prevede una verifica mediante somministrazione di un questionario e

di un test ai docenti per rilevare, analizzare e determinare i diversi livelli raggiunti dopo la formazione e le esperienze degli anni passati, al fine di organizzare nuovi corsi di formazione specifici per consolidare le competenze e/o potenziare quelle già acquisite, anche con l'appoggio della formazione dell'ambito territoriale d'appartenenza.

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.

Nell'ottica di creare ulteriore sinergia fra scuola, studenti/studentesse e famiglie, di promuovere la condivisione di buone pratiche nell'utilizzo consapevole delle TIC e di prevenire e contrastare ogni forma di discriminazione, offesa, denigrazione e lesione della dignità dell'altro, nonché fenomeni di bullismo e cyberbullismo, i docenti dell'Istituto scolastico si impegnano a seguire un percorso formativo specifico ed adeguato che abbia ad oggetto non solo l'uso responsabile e sicuro della Rete ma anche i rischi legati a quest'ultime.
La formazione dei docenti non riguarderà esclusivamente l'alfabetizzazione ai media ma considererà la sfera emotiva e affettiva degli studenti e delle studentesse che usano le nuove tecnologie. Prestare attenzione a questi aspetti significa dare ai docenti gli strumenti per poter educare ragazzi e ragazze alle emozioni in contesto onlife e quindi modulare e gestire i propri ed altrui comportamenti, favorendo e promuovendo forme di convivenza civile.

Il PNSD della scuola ha una progettazione triennale e per questo anno scolastico prevede:

- Incentivazione e sostegno ai docenti sull'uso degli strumenti tecnologici già presenti nella scuola o che si andranno a realizzare e sull'uso di programmi di utilità e online free per testi cooperativi, presentazioni (ppt, ecc…), video e montaggi di foto o mappe e programmi di lettura da utilizzare nella didattica inclusiva.

- Formazione sulle metodologie e sull'uso degli ambienti per la didattica digitale integrata;

- Formazione sull'utilizzo di Learning Managment System;

- Azione di segnalazione di eventi/opportunità formative in ambito digitale, anche utilizzando la formazione d'ambito territoriale;

- Mantenimento dello Sportello di supporto per l'utilizzo delle tecnologie e degli strumenti con l'ausilio degli altri componenti del Team per l'innovazione;

- Proposte della formazione di livello avanzato dei docenti per l'utilizzo della robotica nella didattica, sul coding e sul pensiero computazionale, anche aderendo ad accordi di rete già presenti sul nostro territorio regionale;

- Sistematica informazione, pubblicizzazione e condivisione delle finalità del PNSD con il corpo docente anche per mezzo dell'area dedicata del sito della scuola;

- Ulteriore implementazione dell'utilizzo della piattaforma eTwinning community europea di insegnanti.

- Partecipazione a bandi nazionali, europei e internazionali.

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.

Oggi più che mai è importante rinforzare l'alleanza educativa fra scuola e famiglie.
Il "Patto di Corresponsabilità" è un documento centrale per ogni istituzione scolastica

e per la comunità educante tutta. Al fine di creare una maggiore collaborazione e condivisione degli interventi di formazione e di contrasto al bullismo e al cyberbullismo all'interno della comunità educante, il Patto è stato aggiornato e integrato con il regolamento sul comportamento che gli alunni dovranno adottare nell'uso delle TIC, estratto dal "Piano Scolastico per la didattica digitale integrata" del nostro Istituto. In particolare sono state considerate le modalità di svolgimento delle attività sincrone durante la didattica a distanza, le responsabilità degli studenti e dei genitori e i divieti.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.

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

Scegliere almeno 1 di queste azioni

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.

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.

Nel nostro istituto il trattamento dei dati personali riguarda unicamente le finalità istituzionali per le quali vengono raccolti solo i dati strettamente necessari. Essi sono trattati con o senza l'ausilio di strumenti elettronici e comunque automatizzati secondo le modalità e le cautele previste dalla legge e conservati per il tempo necessario all'espletamento delle attività amministrative e istituzionali.

Il nostro istututo, per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori e all'uso delle tecnologie digitali, ha adottato modelli di liberatoria conformi alla normativa vigente.

3.2 - Accesso ad Internet

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

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure

riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

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

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

Il nostro istituto si è attivato, in modo coerente con il PNSD, per garantire il diritto di accesso a internet anche per quegli studenti che non dispongono della Rete a casa e diffondere una cultura del digitale tale da consentire alla nostra scuola di diventare aperta, flessibile e inclusiva e di adeguarsi ai cambiamenti e alle esigenze della nostra società.

Nel nostro istituto l'accesso ad internet per docenti e studenti è possibile in tutti i plessi attraverso le postazioni fisse presenti nei laboratori e aule multimediali, le LIM in alcune aule o smart TV mobili e un limitato numero di tablet rispetto alla popolazione scolastica.

L'accesso a internet è, inoltre, garantito in tutti gli ambienti amministrativi e dirigenziali dell'istituto e, nella scuola secondaria di primo grado, anche nella biblioteca che dall'anno scorso è stata digitalizzata.

Le specifiche inerenti le limitazioni alla navigazione sono inserite nel Piano per la DDI.

Nei computer presenti nelle aule e nei laboratori sono previsti due profili di accesso con relative password:
 amministratore;
 docente;

È possibile effettuare installazioni e aggiornamenti di software solo tramite la password di amministratore, fornita al personale di assistenza tecnica e all'Animatore Digitale.

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.

L'istituto utilizza le tecnologie digitali per supportare la comunicazione a scuola e facilitare un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale.

A tal fine, l'istituto dispone di un account di posta elettronica istituzionale, utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita e utilizza la piattaforma Argo come registro elettronico e strumento di comunicazione ufficiale con le famiglie.

La comunicazione online è favorita anche dall'utilizzo di mailing list per il personale docente, dal sito ufficiale della scuola e dai social network per l'intera comunità scolastica.

L'utilizzo delle piattaforme digitali Weschool e Bsmart e dei social network nella didattica è contestualizzato ad attività specifiche.Tale utilizzo, reso necessario dalla necessità di rispondere all'emergenza sanitaria legata alla diffusione della pandemia, è regolamentato nel Piano per la DDI.

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.

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno ed influenzano necessariamente anche la didattica e gli stili di apprendimento, ma il loro uso a scuola va disciplinato e regolamentato.

Nel nostro Istituto non è consentito agli alunni di portare a scuola i telefoni cellulari. In caso di urgenza, gli alunni potranno comunicare con le famiglie tramite gli apparecchi telefonici della scuola, su autorizzazione dei docenti e sotto il diretto controllo dei collaboratori scolastici.

Eventuali necessità di detenzione di telefoni cellulari da parte degli alunni devono essere richiesti alla Dirigenza che li autorizzerà solo per gravi e comprovati motivi.

Gli alunni possono tenere i cellulari a scuola ma rigorosamente spenti e riposti negli zaini, anche nell'intervallo. E' inoltre vietato tenere e utilizzare a scuola apparecchi fotografici e similari senza autorizzazione.

La scuola non risponde per eventuali smarrimenti, danneggiamenti o furti di oggetti o strumenti non richiesti dall'attività didattica.

Per il personale docente, durante le ore di lezione è consentito l'uso di dispositivi elettronici personali, unicamente a scopo didattico e a integrazione dei dispositivi scolastici disponibili (computer di classe, tablet della scuola). La detenzione del cellulare è consentita ma il suo uso è limitato alle comunicazioni personali che rivestano carattere di urgenza e comunque non in aula e durante le ore di lezione ma in modo riservato e possibilmente fuori dall'edificio scolastico.

Le famiglie possono in ogni momento prendere contatto con la scuola per eventuali comunicazioni urgenti dirette agli alunni

Durante l'orario di servizio è consentito al personale ATA l'uso del cellulare per comunicazioni personali urgenti. L'uso di altri dispositivi elettronici personali è permesso solo per attività funzionali al servizio, e preventivamente autorizzato.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

- 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 sicuro delle tecnologie digitali (cybersecurity)

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

Scegliere almeno 1 di queste azioni:

- 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 sicuro delle tecnologie digitali (cybersecurity)

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

La nostra scuola, al fine di sviluppare nei ragazzi le competenze, per un utilizzo consapevole delle tecnologie digitali, ha proposto, in questi anni, attività curriculari e progettuali, anche con la presenza di esperti, ed ha promosso la formazione dei docenti.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

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

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

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

Il cyberbullismo è una forma di prepotenza virtuale messa in atto attraverso l'uso di Internet e delle tecnologie digitali. E' "Un atto aggressivo e intenzionale perpetrato da un individuo o da un gruppo, attraverso l'uso delle nuove tecnologie della

comunicazione, in modo ripetuto e continuato nel tempo, contro una vittima che non può facilmente difendersi", secondo la definizione di Smith, del 2006.

Nel bullismo tradizionale, solitamente, la vittima che viene presa di mira è percepita come più debole e incapace di difendersi. Il più forte, quindi, assume atteggiamenti prevaricatori nei confronti del più debole, a partire da una certa "asimmetria di potere".

Ciò, naturalmente, può accadere anche nel caso del cyberbullismo. Mentre nel bullismo tradizionale, però, il potere presenta connotati ben precisi, potrebbe essere, ad esempio, di tipo fisico, legato alla forza o alla statura, o sociale, legato alla popolarità, il potere online può derivare semplicemente dal possesso di specifiche competenze o di alcuni contenuti, come immagini, video, confessioni, che potrebbero essere utilizzati per danneggiare la vittima.

È possibile suddividere gli atti di cyberbullismo in due grandi gruppi: il cyberbullismo diretto, in cui il bullo utilizza strumenti di messaggistica istantanea, che hanno un effetto immediato sulla vittima, poiché diretti esclusivamente a lei, e il cyberbullismo indiretto, in cui il bullo fa uso di spazi pubblici della Rete, come social network, blog, forum, per diffondere contenuti dannosi e diffamatori per la vittima, che possono diventare virali e quindi più pericolosi, anche da un punto di vista psicologico.

È molto importante sottolineare come il cyberbullismo non sia una problematica che riguarda unicamente vittima e cyberbullo. È un fenomeno sociale e di gruppo. Infatti, centrale è il ruolo delle agenzie educative e di socializzazione, formali e informali, più importanti per gli adolescenti: la famiglia, la scuola, i media, le tecnologie digitali e il gruppo dei pari.

Si possono riconoscere i casi di cyberbullismo individuando i seguenti segnali: nervosismo quando si riceve un messaggio o una notifica; essere a disagio nell'andare a scuola o fingere di essere malato; cambiare comportamento in modo repentino; mostrare rabbia o sentirsi depresso; utilizzare sempre meno pc e telefono, arrivando ad evitarli; perdere interesse per le attività familiari ed extrascolastiche; peggioramento del rendimento scolastico.

Chi compie atti di bullismo e cyberbullismo può essere responsabile di reati penali e danni civili.

Le responsabilità per atti di bullismo e cyberbullismo compiute dal minorenne ricadono anche sui genitori, perché devono educare e vigilare, in maniera adeguata all'età del figlio, cercando di correggerne comportamenti devianti; questa responsabilità generale persiste anche per gli atti compiuti nei tempi di affidamento alla scuola (culpa in educando); e sugli insegnanti e la scuola, perché nei periodi in cui il minore viene affidato all'Istituzione scolastica, il docente è responsabile della vigilanza sulle sue azioni e ha il dovere di impedire comportamenti dannosi verso gli altri/e ragazzi/e, insegnanti e personale scolastico o verso le strutture della scuola stessa; la responsabilità si estende anche a viaggi, gite scolastiche, manifestazioni

sportive organizzate dalla scuola (culpa in vigilando). Esiste poi una culpa in organizzando, che si ha quando la scuola non mette in atto le azioni per la prevenzione del fenomeno o per affrontarlo al meglio, così come previsto anche dalla normativa vigente.

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.

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

Certe espressioni di odio sono più estreme, utilizzano termini più insultanti e possono perfino istigare altri ad agire; all'altra estremità della scala, troviamo insulti più moderati o generalizzazioni eccessive, che presentano certi gruppi o individui sotto una cattiva e, perfino, sotto falsa luce.

Può capitare di offendere gli altri senza volerlo, e poi di pentirsi, e perfino di ritirare quanto è stato detto.

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

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

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.

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?

La dipendenza da Internet, come progressivo e totale assorbimento del soggetto alla Rete, può manifestarsi con le seguenti caratteristiche specifiche: la dominanza, che condiziona i pensieri ed il comportamento del soggetto, assumendo un valore primario tra tutti gli interessi; le alterazioni del tono dell'umore, per cui il soggetto prova un aumento d'eccitazione o maggiore rilassatezza, come diretta conseguenza dell'incontro con l'oggetto della dipendenza; il conflitto inter-personale, tra il soggetto e coloro che gli sono vicini, e intra-personale, interno a se stesso; la ricaduta, tendenza a ricominciare l'attività, dopo averla interrotta. Da sottolineare, poi, la nomofobia (nomo deriva da "no-mobile") termine usato per categorizzare quei soggetti che sperimentano emozioni negative, quali ansia, tristezza e rabbia, quando non sono connessi con il proprio smartphone.

Spesso il trascorrere del tempo online, in termini disfunzionali, è scandito dal gioco virtuale, che può anche assumere forme di dipendenza dal gioco online.

La scuola ha la possibilità di indicare strategie, per un uso più consapevole delle tecnologie, finalizzate a favorire il “benessere digitale”, cioè la capacità di creare e mantenere una relazione sana con esse.

Fondamentali sono la ricerca di equilibrio nelle relazioni anche online; l’uso degli strumenti digitali per il raggiungimento di obiettivi personali; la capacità di interagire negli ambienti digitali in modo sicuro e responsabile; la capacità di gestire il sovraccarico informativo e le distrazioni, come le notifiche.

Questo è un argomento trasversale, che può essere affrontato quando si parla di cittadinanza digitale, di cyberbullismo, di uso integrativo e non sostitutivo dei dispositivi e della Rete. La scuola può insegnare molto da questo punto di vista, se integra la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online.

E' importante strutturare regole condivise e stipulare con loro una sorta di “patto” d’aula e, infine, proporre delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d’aula.

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.

Se essi sono sessualmente espliciti, 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. Tra le caratteristiche del fenomeno vi sono principalmente:

- la fiducia tradita: chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario;
- la pervasività con cui si diffondono i contenuti: in pochi istanti e attraverso una condivisione che diventa virale;

- la persistenza del fenomeno: il materiale pubblicato online può permanervi per un tempo illimitato e potrebbe non essere mai definitivamente rimosso.

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.

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.

Potenziali vittime dell'adescamento online possono essere sia bambini che ragazzi. Gli adolescenti sono particolarmente vulnerabili, poiché si trovano in una fase della loro vita in cui è molto importante il processo di costruzione dell'identità sessuale.

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.

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 della sessualità.

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 ragazzi vivono la propria sessualità e la propria immagine online, al loro desiderio di esprimersi e affermare se stessi.

Fondamentale 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.

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.

La pedopornografia esiste da prima dell'avvento di Internet. Tuttavia, la diffusione della Rete, l'evoluzione e la moltiplicazione dei "luoghi" virtuali, il cambiamento costante delle stesse tecnologie digitali, ha radicalmente cambiato il modo in cui il materiale pedopornografico viene prodotto e diffuso, contribuendo ad un aumento della sua disponibilità e dei canali di diffusione.

Studi in materia dimostrano come l'utilizzo di materiale pedopornografico possa essere propedeutico all'abuso sessuale agito ed è quindi fondamentale, in termini preventivi, intervenire per ridurre l'incidenza di tale possibilità.

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. 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.

Il nostro piano d'azioni

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

☐ Promuovere incontri e laboratori per studenti e studentesse dedicati all'

Educazione Civica Digitale.

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

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

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

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.

Ogni qualvolta si ha il sospetto o la certezza che uno/a studente/studentessa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online, bisogna ricordare, innanzitutto, che nell'affrontare quanto accade non si è mai soli. Siamo parte di una comunità scolastica ed è all'interno e con il supporto di essa che il problema va gestito. Per questo, come già sottolineato, nell'ePolicy è importante indicare alcune procedure standardizzate e condivise per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse.

È essenziale che nelle procedure:

- si faccia riferimento a delle figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso;
- sia previsto il coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre che del Dirigente Scolastico.

Sarà cura del dirigente assicurare la massima informazione alle famiglie di tutte le attività e iniziative intraprese, anche attraverso una sezione dedicata sul sito web della scuola, che potrà rimandare al sito del MIUR per tutte le altre informazioni di carattere generale.

Ricordiamo che la Legge 71/2017 indica per la prima volta tempi e modalità per richiedere la rimozione di contenuti ritenuti dannosi per i minori. L'art.2, infatti, prevede che il minore di quattordici anni, ovvero il genitore o altro soggetto esercente la responsabilità sul minore che abbia subito un atto di cyberbullismo, può inoltrare un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi dato personale del minore, diffuso nella rete:

1) al titolare del trattamento
2) al gestore del sito internet
3) al gestore del social media.

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.

E' necessario sottolineare il dovere di sorveglianza dell'insegnante ossia la "culpa in vigilando" attribuibile a chi, nel caso di specie, è tenuto alla vigilanza dei minori che sono affidati al/alla docente.

Ad esempio, in riferimento al cyberbullismo del caso A e caso B citati, si possono seguire le seguenti modalità: nel primo caso si deve coinvolgere innanzitutto il referente d'Istituto per il contrasto del bullismo e del cyberbullismo (e/o il referente indicato nell'ePolicy) valutando insieme le possibili strategie d'intervento. Si potrebbe pensare anche alla possibilità di avvisare l'intero consiglio di classe e, se si ravvisa la necessità e l'urgenza, di coinvolgere il Dirigente Scolastico (considerando il regolamento interno o le prassi già consolidate).

Sarà opportuno (sempre monitorando la situazione) prevedere momenti laboratoriali, utilizzando anche la piattaforma Generazioni Connesse nella parte dei contenuti e dei materiali; tali attività possono essere molto positive, stimolare il dialogo e la riflessione fra gli studenti e le studentesse.

Se i turbamenti osservati si identificano come atti di bullismo o cyberbullismo, il docente e la scuola tutta devono intervenire seguendo la procedura attinente il secondo caso. Il docente deve condividere immediatamente quanto osservato con il referente per il bullismo e il cyberbullismo (e/o il referente indicato nell'ePolicy), valutando insieme le possibili strategie di intervento. Si avvisa anche il Dirigente Scolastico che convoca il consiglio di classe. A seconda della situazione e delle valutazioni effettuate con referente, dirigente e genitori, si potrebbe poi segnalare alla Polizia Postale:

a) contenuto del materiale online offensivo;
b) modalità di diffusione;
c) fattispecie di reato eventuale.

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

5.3. - Gli attori sul territorio

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

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

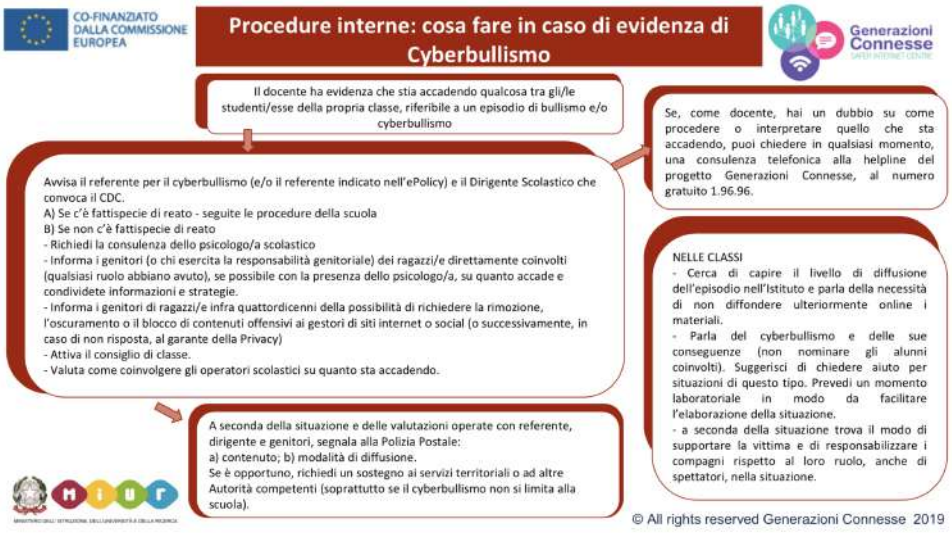
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

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

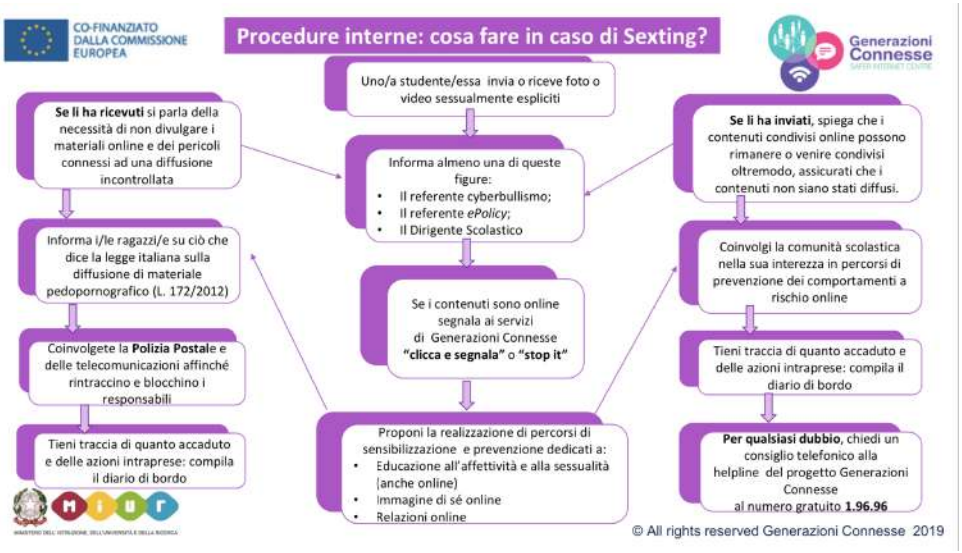
La lista di servizi e istituzioni, indirizzi e recapiti telefonici, a cui fare riferimento, segue una suddivisione regionale, al fine di facilitare l'utilizzatore della guida nell'individuare il servizio più adatto alla problematica che sta affrontando.

5.4. - Allegati con le procedure

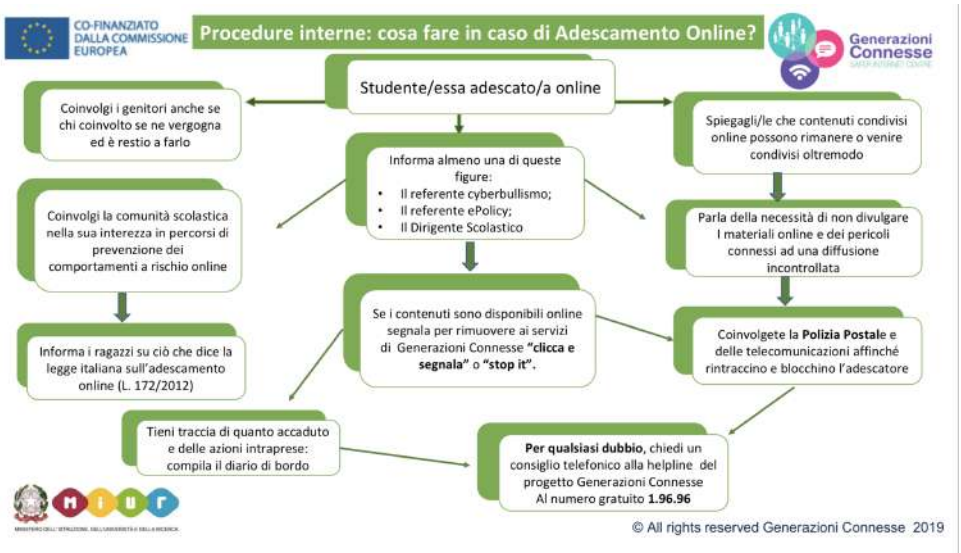
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



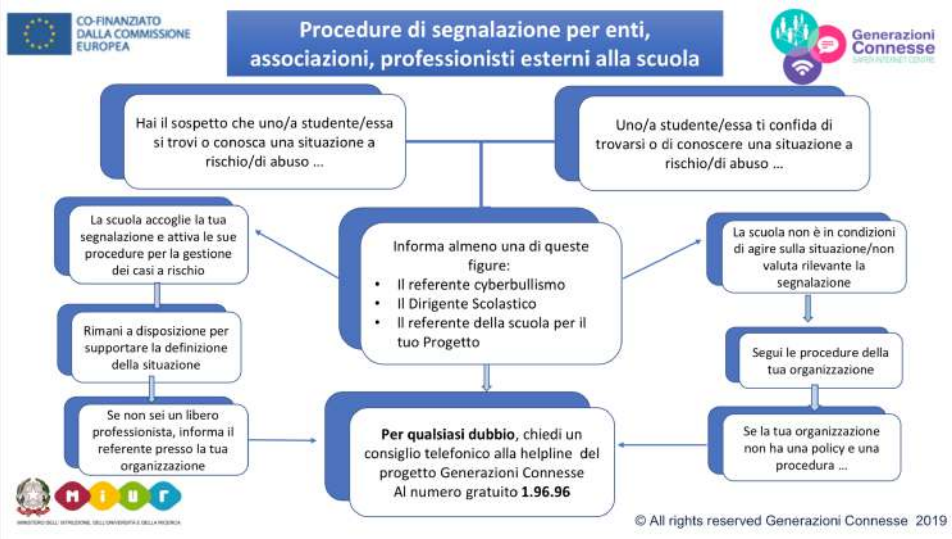
Procedure interne: cosa fare in caso di sexting?



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

Gli schemi su esposti guidano nella scelta delle azioni da intraprendere e indicano le procedure interne da seguire.

Il nostro piano d'azioni

- In caso di problematiche infromare le figure di riferimento preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso;
- avvisare il referente per il contrasto del bullismo, cyberbullismo e Dirigente Scolastico;
- prevedere momenti laboratoriali, utilizzando anche la piattaforma Generazioni Connesse nella parte dei contenuti e dei materiali;
- nei casi più gravi segnalare alla Polizia Postale:

a) contenuto del materiale online offensivo;
b) modalità di diffusione;
c) fattispecie di reato eventuale;

- attività di prevenzione di dialogo 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.