ISTITUTO COMPRENSIVO STATALE - "GREGORIO CALOPRESE"-SCALEA
Prot. 0006768 del 15/06/2026
VI-9 (Uscita)

Documento di ePolicy
IC SCALEA "G. CALOPRESE"

VIA FAZIO DEGLI UBERTI 1 - 87029 - SCALEA
Cosenza (CS) - Calabria
Data di approvazione: 15/06/2026 - 11:27

Cap 1 - Lo scopo della ePolicy

1.1 Scopo della ePolicy

Capitolo 1 - Presentazione dell'ePolicy

1. Scopo dell'ePolicy
2. Ruoli e responsabilità nell'implementazione dell'ePolicy
3. Integrazione dell'ePolicy con regolamenti e normativa generale esistenti
4. Condivisione e comunicazione dell'ePolicy all'intera comunità educante
5. I piani di Azione dell'ePolicy

Capitolo 2 - Sensibilizzazione e prevenzione

1. Sensibilizzazione e prevenzione
2. Il Curricolo Digitale
3. IL KIT DIDATTICO

Capitolo 3 - Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola

1. Protezione dei dati personali e GDPR
2. Accesso ad Internet
3. Strumenti di comunicazione online (PUA)
4. Strumentazione personale (BYOD)

Capitolo 4 - Segnalazione e gestione dei casi

1. Cosa segnalare
2. Come segnalare: quali strumenti e a chi
3. Gli attori sul territorio per intervenire
4. Allegati con le procedure

1.1 Scopo dell'ePolicy

(Questo paragrafo illustra lo scopo e gli obiettivi di questo documento programmatico per la cittadinanza digitale)

L' E-Policy ha come obiettivo principale quello di promuovere le competenze digitali per un uso delle tecnologie digitali positivo, critico e consapevole, da parte degli studenti e delle studentesse guidati dagli adulti coinvolti nel processo didattico-educativo.

La competenza digitale è una competenza chiave del cittadino europeo come indicato dal Consiglio Europeo

(Raccomandazione del 2018) che permette ad ogni cittadino di esercitare i propri diritti all'interno degli ambienti digitali (ONU - Commento Generale 25: I diritti dei minori negli ambienti digitali).

L'ePolicy è un documento programmatico che permette di lavorare su quattro obiettivi:

1. Il piano di azioni triennale per promuovere nell'intera comunità scolastica l'uso sicuro responsabile e positivo della rete;
2. le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
3. le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
4. le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

Attraverso l'aggiornamento dell' ePolicy il nostro Istituto si vuole dotare, dunque, di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio sempre più consapevole, critico ed efficace alla tecnologia, al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.

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

1.2 - ePolicy: ruoli e responsabilità nell'implementazione dell'ePolicy

- (In questo paragrafo vengono dettagliati ruoli e responsabilità nell'implementazione del documento all'interno dei contesti scolastici ivi inclusi rappresentanti genitori e studenti per secondaria II grado).

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

È opportuno che nel documento vengano definiti con chiarezza ruoli, compiti e responsabilità di ciascuna delle figure all'interno dell'Istituto.

In questo paragrafo dell'ePolicy è importante specificare le figure professionali che, a vario titolo, si occupano di gestione e programmazione delle attività formative, didattiche ed educative dell'Istituto e tutte quelle figure appartenenti alla comunità educante.

IL DIRIGENTE SCOLASTICO

Il ruolo del Dirigente Scolastico nel promuovere l'uso consentito delle tecnologie digitali e di internet include i seguenti compiti:

- promuovere la cultura della sicurezza online e garantirla a tutti i membri della comunità scolastica, in linea con il quadro normativo di riferimento, le indicazioni del MIM, delle sue agenzie e attraverso il documento di ePolicy;
- promuovere la cultura della sicurezza online – anche attraverso il documento di ePolicy - integrandola ed inserendola nelle misure di sicurezza più generali dell'intero Istituto;
- ha la responsabilità di fornire sistemi per un uso sicuro delle TIC, internet, i suoi strumenti ed ambienti e deve garantire alla popolazione scolastica la sicurezza di navigazione tramite internet utilizzando adeguati sistemi informatici e filtri;
- ha la responsabilità della gestione dei dati e della sicurezza delle informazioni e garantisce che l'Istituto segue le pratiche migliori possibili nella gestione dei dati stessi;
- deve tutelare la scuola e garantire agli utenti la sicurezza di navigazione utilizzando adeguati sistemi informatici e servizi di filtri Internet;
- ha il compito di garantire a tutto il personale una formazione adeguata sulla sicurezza online per essere tutelato nell'esercizio del proprio ruolo educativo e non;
- deve essere a conoscenza delle procedure da seguire in caso di un grave incidente di sicurezza online;
- deve garantire adeguate valutazioni di rischio nell'usare strumenti e TIC, effettuate in modo che comunque quanto programmato possa soddisfare le istanze educative e didattiche dichiarate nel PTOF di Istituto;
- deve garantire l'esistenza di un sistema che assicuri il monitoraggio e il controllo interno della sicurezza online in collaborazione con le figure di sistema;
- deve essere a conoscenza ed attuare le procedure necessarie in caso di grave incidente di sicurezza online.

L'ANIMATORE DIGITALE E IL TEAM PER L'INNOVAZIONE DIGITALE

L'animatore digitale e il Team per l'Innovazione digitale sono co-responsabili, con il referente ePolicy, dell'attuazione dei piani di azione in particolare in riferimento alla formazione dei docenti. Sono inoltre responsabili del controllo all'accesso da parte degli studenti delle Tic

IL REFERENTE PER IL BULLISMO E CYBERBULLISMO

Il referente cyberbullismo è co-responsabile, con il team ePolicy, dell'attuazione dei piani di azione e coordina le iniziative di prevenzione e contrasto del cyberbullismo.

IL TEAM ANTIBULLISMO E PER L'EMERGENZA

In coerenza con le Linee di Orientamento per la prevenzione e il contrasto del Bullismo e Cyberbullismo del Ministero dell'Istruzione (D.M. n. 18 del 13/1/2021, agg. 2021 – nota prot. 482 del 18-02-2021), il Team ha le funzioni di coadiuvare il Dirigente Scolastico, coordinatore del Team nella scuola, nella definizione degli interventi di prevenzione e nella gestione dei casi di bullismo e cyberbullismo che si possono presentare. Promuove inoltre la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale e comunica ad alunni, famiglie e tutto il personale scolastico dell'esistenza del team, a cui poter fare riferimento per segnalazioni o richieste di informazioni sul tema.

Il Team ha il compito di:

- coadiuvare il Dirigente scolastico, coordinatore del Team, nella definizione degli interventi di prevenzione del bullismo (per questa funzione partecipano anche il presidente del Consiglio d'Istituto e i Rappresentanti degli

studenti).

- Intervenire (come gruppo ristretto, composto da Dirigente e referente o referenti per il bullismo e il cyberbullismo, psicologo o pedagogista, se presente) nelle situazioni acute di bullismo.
- Promuovere la redazione e l'applicazione della ePolicy e monitorare le segnalazioni.

I/LE DOCENTI

I/le docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete. Possono, innanzitutto, integrare la propria disciplina con approfondimenti, promuovendo l'uso delle tecnologie digitali nella didattica. I docenti devono accompagnare e supportare gli/le studenti nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete. Inoltre, educano gli studenti alla prudenza, a non fornire dati ed informazioni personali, ad abbandonare un sito dai contenuti che possono turbare o spaventare e a non incontrare persone conosciute in Rete senza averne prima parlato con i genitori. Informano gli alunni sui rischi presenti in Rete, senza demonizzarla, ma sollecitandone un uso consapevole, in modo che Internet possa rimanere per bambini/e e ragazzi/e una fonte di divertimento e uno strumento di apprendimento.

I/le docenti osservano altresì regolarmente i comportamenti a rischio (sia dei potenziali bulli, sia delle potenziali vittime) e hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che veda coinvolti studenti e studentesse dandone tempestiva comunicazione al Dirigente Scolastico, al Referente per il Cyberbullismo e Bullismo e al Consiglio di Classe per definire strategie di intervento condivise.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Responsabile della protezione dei dati (RPD o DPO) conosce l'ePolicy di Istituto, fornisce la propria consulenza in merito agli obblighi derivanti dal GDPR e sorveglia sull'esatta osservanza della normativa in materia di tutela dei dati personali ed è co-responsabile delle azioni di informazione e formazione nell'Istituto sulla protezione dei dati personali

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

Il personale ATA, all'interno dei singoli regolamenti d'Istituto, è coinvolto nelle pratiche di prevenzione – ivi incluso il processo di definizione e implementazione dell'ePolicy di Istituto - ed è tenuto alla segnalazione di comportamenti non adeguati e/o episodi 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 dovrebbero imparare a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le. Affinché questo accada devono partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education.

I rappresentanti degli/delle studenti sono informati del documento di ePolicy e invitati a costruire i piani di azione, a partire dal secondo anno della secondaria di II grado,

I GENITORI/ADULTI DI RIFERIMENTO

I Genitori, in continuità con l'Istituto scolastico, sono attori partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile degli strumenti personali (pc, smartphone, etc). Come parte della comunità educante sono tenuti a relazionarsi in modo costruttivo con i/le docenti sulle linee educative che riguardano le TIC e la Rete e – ivi incluso il documento di ePolicy - comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet.

È estremamente importante che accettino e condividano quanto scritto nell'ePolicy d'Istituto e nel patto di corresponsabilità in un'ottica di collaborazione reciproca. Si promuove il coinvolgimento dei rappresentanti di genitori/adulti di riferimento all'interno del percorso di definizione e implementazione dell'ePolicy.

GLI ENTI ESTERNI PUBBLICI E PRIVATI E LE ASSOCIAZIONI

Enti esterni pubblici e privati, il mondo dell'associazionismo dovranno conformarsi alla politica della scuola riguardo all'uso consapevole delle TIC e della rete per la realizzazione di iniziative nelle scuole, finalizzate a promuovere un uso positivo e consapevole delle Tecnologie Digitali da parte dei più giovani, e/o finalizzate a prevenire e contrastare situazioni di rischio online e valutare la rispondenza delle proposte di attività di sensibilizzazione/formazione alle esigenze di qualità contenute nel documento di ePolicy. Dovranno inoltre promuovere comportamenti sicuri durante le attività che si svolgono con gli/le studenti e verificare di aver implementato una serie di misure volte a garantire la tutela dei minori nel caso di insorgenza di problematiche e ad assicurarne la tempestiva individuazione e presa in carico.

La scuola coglierà ogni occasione per sensibilizzare studenti e i genitori attraverso incontri con la Polizia municipale ed altri esperti o educatori, circolari, sito web e altre comunicazioni telematiche, informazioni su campagne di sicurezza promosse da altre istituzioni o su convegni dedicati a questo tema. I genitori saranno incoraggiati a sostenere la scuola nel promuovere le buone pratiche digitali e a seguire le linee guida sull'uso appropriato di immagini e video registrati in occasione di eventi scolastici – anche al di fuori delle aule – nonché accesso alle sezioni del sito dedicate ai genitori, con particolare riguardo al registro elettronico e agli ambienti virtuali istituzionali.

UN'INFORMATIVA PER I SOGGETTI ESTERNI CHE EROGANO ATTIVITÀ EDUCATIVE NELL'ISTITUTO

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

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

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

1.3 Integrazione ePolicy nei documenti scolastici

(Il paragrafo spiega in che modo integrare il documento nel Regolamento dell'Istituto Scolastico da aggiornare con specifici riferimenti all'E-policy, così come nel RAV e all'interno del Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto).

La trasversalità dell'ePolicy rende necessaria una sua integrazione nell'ambito dei documenti che disciplinano il funzionamento dell'Istituto Scolastico.

Il Regolamento dell'Istituto scolastico, che rappresenta il principale punto di riferimento normativo, dovrà essere aggiornato in modo tale da dare contezza dell'adozione dell'ePolicy, e richiamare le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione in ambiente scolastico.

Anche il **Patto di Corresponsabilità educativa** tra scuola e famiglia dovrà essere integrato con gli opportuni riferimenti all'ePolicy, puntualizzando, da un lato l'impegno dell'Istituto ad organizzare eventi formativi/informativi a beneficio dei genitori, e dall'altro l'impegno di questi ultimi a partecipare in maniera proattiva a tali eventi.

Il **Piano Triennale dell'Offerta Formativa**, per la sua funzione di carta d'identità culturale e progettuale delle istituzioni scolastiche, nel quale si esplicita la progettazione curricolare, extracurricolare, educativa e organizzativa che le singole scuole adottano nell'ambito della loro autonomia, deve contenere anche le progettualità relative ad azioni media educative legate al percorso di ePolicy.

Così come il PTOF è il risultato di una consapevole concertazione fra le componenti delle istituzioni scolastiche (Dirigente Scolastico, docenti, alunni, genitori) e fra queste e il territorio, il patto di corresponsabilità rappresenta l'assunzione di responsabilità da parte di tutti coloro che svolgono un ruolo attivo nella Comunità educante.

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

1. il curricolo sulle competenze digitali per la comunità educante (il DigComp2.2);
2. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con relative informative;
3. Come comunicare e condividere l'epolicy con gli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).

1. Informazione della comunità educante (in particolare le famiglie) sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali con relative informative;

L'efficacia dell'ePolicy è direttamente proporzionale a livello di conoscenza e diffusione all'interno della comunità scolastica ivi comprese le famiglie. Il documento rappresenta il canale interno privilegiato per informare, responsabilizzare e collaborare sui temi della rete e delle tecnologie a scuola con l'intera comunità scolastica.

In tal senso, il documento è accompagnato da versioni, allegate e sintetiche, all'interno delle quali sono individuati gli elementi principali del documento; una versione è diretta agli studenti ed una è diretta alle famiglie con un linguaggio e una presentazione dei contenuti adeguata, flessibile e chiara. La versione sintetica rivolta agli studenti è inserita all'interno delle attività didattiche dell'educazione alla cittadinanza mentre la versione per le famiglie è consegnata nel corso dei colloqui scuola-famiglia.

Il documento è altresì pubblicato sul sito della scuola ed inserito nel Patto di corresponsabilità.

2. Come comunicare e condividere l'ePolicy con gli attori pubblici e privati (enti, aziende, associazioni, etc) che realizzano iniziative nelle scuole sui temi dell'educazione civica digitale con relative informative).

La presenza dell'ePolicy nell'Istituto scolastico è garanzia, per il territorio, della presenza di un presidio informato, sensibile e attento sulla rete e le tecnologie in relazione con i più giovani.

In questo senso l'Istituto può rappresentare per le Istituzioni del territorio, le aziende, e le realtà del Terzo Settore un luogo di confronto privilegiato e di sperimentazione per tutti coloro che intendono costruire progetti di cittadinanza digitale rivolte ai più giovani.

A tal fine l'adozione dell'ePolicy è comunicata all'USR di riferimento e al Municipio (servizi istruzione e servizi sociali) attraverso gli allegati sintetici progettati che indicano gli elementi del documento e le prospettive per la comunità.

Il documento di E-policy, come indicato in precedenza, dunque, verrà condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. Il documento, dopo l'approvazione da parte del Collegio dei Docenti e del Consiglio di Istituto, sarà esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque in vari punti spaziali dell'Istituto.

L' ePolicy verrà condivisa e comunicata a tutta la 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;
- l'insegnamento trasversale di educazione civica.

Gli studenti e le studentesse verranno informati sul fatto che sono monitorati e supportati nella navigazione online, negli spazi della scuola e sulle regole di condotta da tenere in Rete, in modo da fornire loro norme condivise di sicurezza e prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e.

Ciascun attore scolastico (dai docenti agli/lle studenti/esse) si farà a sua volta promotore del documento in relazione al proprio ruolo.

I docenti, ai quali saranno riservati anche i corsi di Generazioni Connesse, potranno confrontarsi sui contenuti, sulle pratiche indicate e su come inserire nel curricolo le tematiche di interesse per poi elaborare miglioramenti alla policy vigente.

Per i genitori saranno organizzati incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare anche in collaborazione con gli enti del territorio e i progetti indicati nel PTOF.

GESTIONE DELLE INFRAZIONI ALLA EPOLICY

La scuola gestirà le infrazioni all'ePolicy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni. Gli interventi previsti per gli alunni sono rapportati all'età e al livello di sviluppo dell'alunno. Più gli alunni sono piccoli, infatti, più i comportamenti "da correggere" sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, che devono essere compresi e orientati proprio dagli educatori, nella prospettiva del raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno.

Sono previsti pertanto provvedimenti disciplinari proporzionati all'età e alla gravità del comportamento.

a) SANZIONI DECISE DAL SINGOLO DOCENTE:

- il richiamo verbale;
- invito alla riflessione individuale;
- consegna da svolgere in classe significativa e commisurata;
- sospensione temporanea delle attività ludiche dell'intervallo;
- ammonizione scritta sul libretto personale o quaderno delle comunicazioni;
- ammonizione scritta sul registro di classe e riportata sul libretto personale o quaderno delle
- comunicazioni, eventualmente controfirmata dal Dirigente Scolastico.

b) SANZIONI DECISE DAL CONSIGLIO DI CLASSE SENTITO IL PARERE DEL DIRIGENTE SCOLASTICO:

- Ammonizione scritta ufficiale da parte del Dirigente Scolastico;
- Diffida scritta con comunicazione alla famiglia da parte del Dirigente Scolastico;
- Sospensione delle visite guidate, viaggi d'istruzione, gruppi sportivi o altre attività con l'obbligo della
- presenza a scuola con altre mansioni concordate;
- sospensione delle lezioni con o senza obbligo di frequenza fino a tre giorni;
- sospensione delle lezioni con o senza obbligo di frequenza fino a quindici giorni;
- sospensione oltre i quindici giorni solo nel caso di fatti di rilevanza penale o pericolo per l'incolumità
- delle persone tali da richiedere l'intervento degli Organi Istituzionali di Competenza.

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

Per quanto riguarda il personale scolastico, esso è tenuto ad un uso responsabile e adeguato delle TIC e dei servizi della scuola, rispettando la normativa vigente in relazione al trattamento dei dati personali, comuni e sensibili degli alunni, la segretezza delle password e la custodia degli strumenti e degli accessi di cui possono approfittare terzi. Tutto il personale è tenuto a collaborare con il Dirigente Scolastico e a fornire ogni informazione utile per le valutazioni di singoli casi in cui vi è il sospetto di una violazione delle norme indicare, nonché per l'avvio di procedimenti che possono avere carattere organizzativo-gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

In considerazione dell'età dei discenti, le azioni e la condotta dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola e, pertanto, i genitori degli alunni possono essere convocati a scuola per concordare misure educative sanzionatorie anche a norma di legge.

1.5 - I Piani di Azione dell'ePolicy

I piani di azione rappresentano il **programma triennale** di obiettivi che la scuola intende realizzare per promuovere la conoscenza delle regole e dei protocolli di intervento che sono stati adottati con il documento di ePolicy nella comunità scolastica.

Nei Piani di Azione sono riportati **gli impegni e le responsabilità** che la scuola si assume per promuovere sui temi dell'educazione civica digitale e dell'utilizzo sicuro e consapevole delle tecnologie e della rete:

- la rilevazione dei bisogni
- le iniziative informative e formative,
- la formazione di docenti, studenti e studentesse, e famiglie,
- il monitoraggio e la valutazione delle azioni (laddove possibile, anche all'interno del RAV);

I Piani di Azione si distinguono tra standard, comuni ad ogni scuola che ha adottato l'ePolicy, e autoprodotti ovvero definiti dalla scuola sulla base del proprio contesto territoriale e delle collaborazioni in essere con Istituzioni, associazioni e aziende.

1° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

- Realizzare un evento di presentazione dell'ePolicy ai docenti dell'Istituto;
- Realizzare un evento di diffusione dell'ePolicy in occasione degli Open Day e/o in occasione del SID dell'Istituto dedicato alle famiglie ed a studenti/esse;
- Diffondere l'ePolicy negli ambienti scolastici, a studenti e studentesse, docenti e famiglie attraverso le versioni friendly dell'ePolicy;

MODULO II

- Effettuare una rilevazione del fabbisogno formativo dei docenti sui temi dell'educazione civica digitale;
- Effettuare una rilevazione di interessi, bisogni e comportamenti delle famiglie sull' uso positivo del digitale;
- Avviare l'introduzione dell kit didattico come metodo e risorsa di lavoro in alcune classi pilota;

MODULO III

- Integrare l'ePolicy (norme, regolamenti e procedure) nei documenti dell'Istituto;
- Aggiornare la Politica d'Uso Accettabile (PUA) della scuola ed il regolamento BYOD dell'Istituto;

MODULO IV

- Definizione, a partire da quanto definito nell'ePolicy, delle procedure di segnalazione anche con linguaggio child/youth friendly perché possano essere accessibili a studenti e studentesse;
- Realizzare una reportistica delle segnalazioni ricevute e dei relativi esiti.

2° ANNO DI ATTIVITA' CON L'EPOLICY

MODULO I

- Realizzare una formazione rivolta ai docenti dell'Istituto, sulla base dei risultati della rilevazione svolta nel corso del primo anno, anche attraverso il supporto di esperti/associazioni esterne o avvalendosi del percorso disponibile sul sito di Generazioni Connesse. La formazione deve coprire almeno il 60% del corpo docente.

MODULO II

- L'istituto utilizza il kit didattico come pratica metodologica e risorse a disposizione dei docenti per i percorsi di ECD attraverso la formazione specifica sviluppata per i docenti attraverso il sito di Generazioni Connesse;
- Effettuare una rilevazione di interessi, bisogni, comportamenti, abitudini di studenti e studentesse sui temi dell'educazione civica digitale;
- Realizzare una formazione rivolta agli studenti e alle studentesse attraverso il percorso previsto sulla piattaforma di Generazioni Connesse;
- Realizzare una formazione rivolta alle famiglie attraverso il percorso previsto sulla piattaforma di Generazioni Connesse

MONITORAGGIO DELL'IMPLEMENTAZIONE DELLA POLICY E SUO AGGIORNAMENTO

L'Istituto svolgerà, inoltre, in maniera periodica Il monitoraggio dell'implementazione della Policy e tale monitoraggio sarà curato dal Dirigente Scolastico con la collaborazione dell'Animatore digitale, del responsabile ePolicy, del referente Bullismo e Cyberbullismo, nonché del Team Antibullismo e dai docenti delle classi tramite questionari e conversazioni. L' attività sarà volta a rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di internet. Il monitoraggio sarà rivolto anche agli insegnanti, al fine di valutare l'impatto della policy e la necessità di eventuali miglioramenti.

1.6 - Le risorse di Generazioni Connesse

Risorse di Generazioni Connesse:

- Kit Didattico
- Area formazione (per docenti, famiglie, studenti/sse con ePolicy)
- Canale Youtube (webinar, video-stimolo, serie per target differenti)
- Canale TikTok
- Canale Instagram
- Canale Facebook

Il nostro Istituto si avvale di tutti gli strumenti forniti da Generazioni Connesse con una selezione delle attività in base alle diverse fasce di età.

Cap 2 - Sensibilizzazione e prevenzione

2.1 - Sensibilizzazione e prevenzione

(Il capitolo raccoglie indicazioni su azioni formative per studenti/esse, famiglie e docenti con obiettivi a breve e lungo termine e riferimenti normativi (es legge 92 2019 su ECD). I rischi online andranno in appendice come glossario, sul sito come approfondimenti, sul kit didattico come attività.

La quotidianità in rete di ciascuno dei componenti della comunità scolastica - docenti, studenti e famiglie - deve essere caratterizzata da una consapevolezza critica delle caratteristiche degli ambienti e dei servizi online affiancata alle competenze per vivere al meglio il mondo connesso.

In questa direzione l'ePolicy è un documento che sviluppa azioni e interventi con l'obiettivo di raggiungere l'intera comunità scolastica e promuovere, ciascuno secondo il proprio ruolo, una cittadinanza digitale composta dalla conoscenza dei diritti in rete, dei rischi e delle opportunità per una partecipazione attiva e responsabile nella rete.

Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

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 il sito web dell'Istituto.

Allo scopo di mantenere viva l'attenzione delle famiglie su tali temi verranno valorizzate, inoltre, le opportunità di incontro e formazione per le famiglie sui temi oggetto della Policy, offerte dal territorio, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità.

Il coinvolgimento dell'intera Comunità scolastica è parte integrante del PTOF ed è una delle misure individuate nel Piano d'azione proposto a "Generazioni Connesse".

Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di smartphone, chat line e social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo.

2.2 - Il Curricolo Digitale

Per realizzare questo obiettivo l'istituto utilizza le risorse messe a disposizione a livello nazionale e internazionale.

Il DigComp 2.2, framework europeo sulle competenze digitali, permette di costruire una cornice precisa in cui inquadrare i temi e le corrispondenti competenze da proporre nell' Istituto non solo per gli studenti.

Al suo interno vengono identificati alcuni temi sui quali è costruita una proposta specifica per le famiglie e gli studenti

(formazione). Tale cornice trova poi sviluppo specifico, per gli studenti, nel curricolo di educazione alla Cittadinanza Digitale previsto dalla L. 92/2019. Il curricolo prende forma attorno all'ePolicy e le attività didattiche sono legate al documento ed alle scelte dell'Istituto al suo interno.

Nel curricolo va previsto in ogni classe un appuntamento didattico specifico, calibrato sull'età degli alunni, e l'utilizzo dei kit didattici per favorire da parte degli studenti una maggiore conoscenza e consapevolezza delle finalità del presente documento.

I regolamenti e le attività sviluppate sul tema della prevenzione presenti nell'ePolicy sono parte, costante ma non esclusiva, delle azioni di disseminazione e sensibilizzazione descritte ed attuate dall'Istituto.

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 e consolidate 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. Il nostro Istituto, infatti, in relazione alla competenza digitale, prevede le seguenti conoscenze, abilità, nonché atteggiamenti:

Competenza digitale	
Conoscenze	Comprendere in che modo le tecnologie digitali possono essere di aiuto alla comunicazione, alla creatività e all'innovazione, pur nella consapevolezza di quanto ne consegue in termini di opportunità, limiti, effetti e rischi. Comprendere i principi generali, i meccanismi e la logica che sottendono alle tecnologie digitali in evoluzione. Conoscere il funzionamento e l'utilizzo di base di diversi dispositivi, software e reti. Assumere un approccio critico nei confronti della validità, dell'affidabilità e dell'impatto delle informazioni e dei dati resi disponibili con strumenti digitali. Essere consapevoli dei principi etici e legali chiamati in causa con l'utilizzo delle tecnologie digitali.
Abilità	Essere in grado di utilizzare le tecnologie digitali come ausilio per la cittadinanza attiva e l'inclusione sociale, la collaborazione con gli altri e la creatività nel raggiungimento di obiettivi personali, sociali o commerciali. Utilizzare, accedere a, filtrare, valutare, creare, programmare e condividere contenuti digitali. Essere in grado di gestire e proteggere informazioni, contenuti, dati e identità digitali. Riconoscere software, dispositivi, intelligenza artificiale o robot e interagire efficacemente con essi.
Atteggiamenti	Atteggiamento riflessivo e critico, ma anche improntato alla curiosità, aperto e interessato al futuro della loro evoluzione. Approccio etico, sicuro e responsabile all'utilizzo di tali strumenti.

L'uso consapevole e responsabile delle tecnologie digitali, in particolar modo in contesti didattici nuovi (vedi anche le

precendenti DAD e DDI), richiede una costante e attenta progettazione/implementazione del curricolo digitale, continuativo e trasversale alle varie discipline ed elaborato in relazione al target di riferimento (ordine e grado, classi, etc.), allo scopo di:

- far riflettere gli alunni sul potenziale delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana, allo scopo di evitare automatismi e di conseguenza atteggiamenti e comportamenti incerti. Per tale motivo si lavorerà sull'adeguata comprensione della 'grammatica' dello strumento (dimensione tecnologica);
- sviluppare nei discenti la capacità di ricercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità (dimensione cognitiva);
- far assumere atteggiamenti responsabili in relazione sia ai dati personali che altrui, usando le tecnologie per scopi eticamente accettabili e sempre nell'ottica del rispetto per gli altri (dimensione etica);
- far acquisire buone pratiche sociali e, pertanto, rafforzare e potenziare le abilità socio-comunicative e partecipative per maturare una consapevolezza maggiore sui doveri nei riguardi di coloro con cui si comunica online (dimensione sociale).

Proprio lo sviluppo della dimensione tecnologica, cognitiva, etica e sociale permette di raggiungere le competenze digitali, intese come competenze chiave, che al termine del percorso scolastico vengono individuate e certificate coerentemente con quanto normato dalla C.M. n 3, prot. n. 1235 del 13 febbraio 2015, il cui livello raggiunto è identificato dai seguenti dagli indicatori:

Livello	Indicatori esplicativi
A – Avanzato	L'alunno/a svolge compiti e risolve problemi complessi, mostrando padronanza nell'uso delle conoscenze e delle abilità; propone e sostiene le proprie opinioni e assume in modo responsabile decisioni consapevoli.
B – Intermedio	L'alunno/a svolge compiti e risolve problemi in situazioni nuove, compie scelte consapevoli, mostrando di saper utilizzare le conoscenze e le abilità acquisite.
C – Base	L'alunno/a svolge compiti semplici anche in situazioni nuove, mostrando di possedere conoscenze e abilità fondamentali e di saper applicare basilari regole e procedure apprese.
D – Iniziale	L'alunno/a, se opportunamente guidato/a, svolge compiti semplici in situazioni note.

Tutte le azioni attivate dal nostro Istituto per l'implemento del curricolo e delle competenze digitali hanno fatto riferimento ai seguenti documenti:

- Piano Scuola Digitale (PNSD);
- Sillabo sull'Educazione Civica Digitale;
- Dig.Com 2.1.: 'Il quadro di riferimento per le competenze digitali dei cittadini';
- Raccomandazione del Consiglio Europeo relative alle competenze chiave per l'apprendimento (C189/9, p. 9);
- Legge n. 92 del 20 agosto 2019: "Introduzione dell'insegnamento dell'educazione civica" (in particolar modo art. 5);
- Linee guida per l'insegnamento dell'educazione civica. Allegati A-B (22-06-2020).

Il curricolo digitale e l'offerta dell'Istituto, inoltre, si basa sui seguenti nuovi riferimenti europei e nazionali:

- DigComp 2.2: Aggiornamento del framework per le competenze digitali dei cittadini con focus su Intelligenza Artificiale e lavoro agile;
- DigCompEdu: Il quadro di riferimento europeo fondamentale per le competenze;
- Piano Scuola 4.0 (DM 218/2022);
- Linee Guida per le Competenze STEM e Digitali (DM 184/2023): Direttive per integrare le discipline scientifiche e digitali in tutti i cicli scolastici;
- Nuove Linee Guida per l'Insegnamento dell'Educazione Civica (DM 183/2024): che sostituiscono le linee guida del 2020 e aggiornano la cittadinanza digitale;
- DM 65/2023: 'Digital Teacher';
- Regolamento sull'utilizzo dell'Intelligenza Artificiale (IA).

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.

La formazione del corpo docente verrà organizzata su due livelli: interno ed esterno. A livello interno, nel PTOF si prevede che una parte della formazione in servizio obbligatoria ai sensi della L.107/2015 sia dedicata proprio all'uso e al potenziamento delle TIC nella didattica e ai temi informatici in generale. Tale formazione è svolta dall'animatore digitale e dai docenti dell'Istituto presenti nella scuola che negli anni hanno maturato conoscenze e competenze didattico-metodologiche. Tutto il corpo docente riceverà l'assistenza, gli strumenti e i mezzi per poter mettere in pratica una didattica innovativa mediante le nuove tecnologie anche attraverso le potenzialità della piattaforma Google Workspace.

Per quanto riguarda la formazione esterna, la scuola assicura tempestiva e capillare informazione su corsi, convegni e seminari relativi a tali argomenti e continuerà ad assicurare la formazione specifica sull'utilizzo delle TIC nella didattica anche attraverso i corsi organizzati dall'istituzione, dalle scuole associate nella rete dell'ambito di appartenenza.

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 (come Generazioni Connesse) allo scopo di prevenire e contrastare ogni forma di discriminazione, offesa, denigrazione e lesione della dignità dell'altro, nonché bullismo e cyberbullismo. 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 team per il contrasto del 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.

2.3 - Il Kit Didattico

L'e-Policy prevede, a livello macro, un lavoro di lettura e d'intenti condivisi dall'intera comunità scolastica, a livello micro, invece, immagina che la singola classe lavori anche su tematiche direttamente collegate alla sicurezza in rete, ma complesse e di non immediata ricaduta nelle programmazioni scolastiche (etica e digitale, algoritmi, datafication). A tal fine si è progettato e predisposto del materiale che possa funzionare sia da attivatore, sia d'accompagnamento ai docenti e agli studenti nella fase più delicata ed incisiva del processo di prevenzione: la lezione in classe.

Pertanto, il progetto Generazioni Connesse, a supporto del lavoro dell'e-Policy ha previsto per i docenti e studenti di ogni segmento scolare un nuovo Kit Didattico che contiene materiali per le lezioni e per il proprio aggiornamento, a partire dalla scuola d'infanzia fino alla secondaria di secondo grado. Il Kit può essere usato nella sua interezza oppure può essere oggetto di selezione e scelta, sulla base di quanto fatto dal docente.

Cap 3 - Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola

3.1 - Protezione dei dati personali e GDPR

La protezione dei dati personali delle persone fisiche costituisce un diritto fondamentale. L'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea e l'art. 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Le principali normative di riferimento sono il Regolamento Generale sulla Protezione dei Dati 2016/679 noto anche come GDPR, e il Dlgs 196/2003 conosciuto come Codice Privacy.

Il settore dell'istruzione è particolarmente impattato dalla tematica privacy in considerazione del fatto che gli Istituti Scolastici sono chiamati, necessariamente, a trattare un'enorme mole di dati personali.

Con l'entrata in vigore del GDPR è stato introdotto l'obbligo per ciascun Istituto scolastico di provvedere alla designazione di un Responsabile della protezione dei dati personali (RPD o DPO).

I principali obblighi in materia di protezione dei dati personali consistono nella definizione di un "organigramma privacy", nel rilascio dell'informativa al momento della raccolta dei dati e nella tenuta di un registro dei trattamenti.

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, come detto in precedenza, 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 nostra scuola, pertanto, già adeguatasi al GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, si impegna a tutelare la privacy degli/lle studenti/esse e delle loro famiglie, nonché di rendere consapevoli gli studenti e le studentesse dell'importanza del diritto alla riservatezza di se stessi e degli altri. Per tale motivo, dunque, il nostro Istituto segue la normativa prevista per il trattamento dati in relazione alle specifiche finalità istituzionali e alle specifiche norme di legge e si impegna a migliorare la sicurezza e potenziare la protezione dei dati trattati attraverso un'attenta formazione dei responsabili, degli incaricati ed eventualmente sub-incaricati del trattamento, nonché delle figure coinvolte nel processo educativo.

3.2 - Strumenti di comunicazione online (PUA)

La Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) è un documento che racchiude una serie di regole legate all'utilizzo della rete a scuola e a casa da parte di studenti e di tutto il personale (compresi i professionisti esterni che lavorano in contesto scolastico), integrante il DPS (Documento programmatico sulla Sicurezza). Il documento, che funge da raccordo, si compone di punti strategici riguardanti non solo i vantaggi di internet a scuola ma anche i rischi connessi all'online, nella valutazione di quei contenuti presenti in rete e di quelle azioni negative che possono comprometterne l'uso positivo. Fra queste attività: ricercare materiale non consono allo stile educativo della scuola; produrre vere e proprie azioni illecite; giocare online con la rete scolastica; violare la privacy e i diritti d'autore, etc... Nella Politica d'Uso Accettabile e Responsabile della Rete (P.U.A.) vengono definite, dunque, le regole di utilizzo fra tutti gli attori in gioco, nel rispetto dei dati sensibili di ciascuno, in particolar modo degli alunni e delle alunne.

Accesso ad internet

- L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.
- 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.
- Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.
- L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.
- 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.

Per questo motivo il nostro Istituto è attento a queste tematiche e si impegna a realizzare e potenziare tutte le attività e procedure per creare ambienti di apprendimento con le caratteristiche indicate, partecipando, infatti, a bandi di implementazione e strumentazione, ad esempio, per le classi virtuali.

Nel particolare, la nostra scuola è dotata di:

- accesso internet in tutte le classi attraverso una rete WI-FI adeguata al numero di studenti e in grado di supportare il traffico dati generato da un numero elevato di utenti (gli alunni possono usufruire della connessione solo tramite pc);

- connessione ad internet tramite collegamento wireless. La Dirigenza e l'Amministrazione hanno una rete separata;

- connessione in tutte le aree della scuola;

- laboratori di informatica con software di controllo gestito dal docente.

Per quanto riguarda l'accesso ad internet, filtri, antivirus e navigazione, il nostro Istituto presenta un proxy server per monitorare il traffico web e per bloccare l'accesso a siti inappropriati a un contesto scolastico.

Occorre, inoltre, sensibilizzare tutta la comunità scolastica sull'opportunità di mantenere aggiornati gli antivirus installati sulle macchine personali e controllare i dispositivi di archiviazione esterna che vengano collegati al proprio pc.

Google workspace

L'Istituto "G.Caloprese" ha attivato, inoltre, i servizi della piattaforma Google Workspace che proprio Google mette gratuitamente a disposizione delle scuole e delle università. Questo spazio è costituito da un insieme di applicazioni (la posta elettronica, documenti condivisi (Google drive), calendario, siti web (Sites) e Google Classroom (classi virtuali). Con la piattaforma Workspace la proprietà dei dati rimane in capo all'utente, con totale protezione e privacy e priva di pubblicità, mentre per gli account privati le possibilità di "intromissione" da parte di Google sono numerose. L'obiettivo di questa iniziativa è ottimizzare, attraverso le tecnologie di rete, l'attività didattica e la circolazione delle informazioni interne, come comunicazioni, documentazione e didattica (tramite uso di applicazioni specifiche). le attività di Google Workspace consentono di gestire in modo efficace il flusso informativo all'interno dell'istituto attraverso tre strumenti principali e relative applicazioni:

- Comunicazione: Gmail, Meet, Hangouts, Calendar,gruppi Google+
- Archiviazione: Drive
- Collaborazione: Condivisione di Documenti,fogli, presentazioni, moduli, Sites e di Google Classroom per la gestione di una classe virtuale.
- ad ogni studente è stato assegnato una casella postale composta dall'iniziale del proprio nome, cognome, seguita dal nome di dominio della scuola, esempio: ncognome@icscalea.edu.it

Gli studenti, già durante la DAD, hanno utilizzato la casella di posta all'interno del dominio @icscalea.edu.it e ad uso esclusivo per le attività della scuola,l'Istituto continua ad utilizzare i servizi offerti da Google Workspace e ad integrarli costantemente nella didattica quotidiana

Per lavorare bene insieme si sono stabilite ovviamente delle regole di comportamento rese note attraverso la relativa liberatoria. Lo studente, infatti, riceverà la password per accedere ai servizi di Google Workspace, solo quando lui e un suo genitore/tutore avranno sottoscritto e riconsegnato agli insegnanti le regole di utilizzo, dichiarando così di averle accettate e di essere a conoscenza della normativa locale, nazionale ed europea vigente. È solo in tal modo che lo studente avrà accesso alla piattaforma di Google Workspace. Lo studente si impegna:

- a conservare la password personale e a non consentire l'uso ad altre persone;
- a comunicare immediatamente attraverso email a admin@icscalea.edu.it l'impossibilità di accedere al proprio account o il sospetto che altri possano accedervi;
- a non consentire ad altri, a nessun titolo, l'utilizzo della piattaforma Google Suite for Education;
- a non diffondere eventuali informazioni riservate di cui venissero a conoscenza,relative all'attività delle altre persone che utilizzano il servizio;
- ad osservare il regolamento,pena la sospensione da parte dell'Istituto dell'account personale dello studente,
- ad utilizzare i servizi offerti solo ad uso esclusivo per le attività didattiche della scuola.

Lo studente e la sua famiglia si assumono la piena responsabilità di tutti i dati da lui inoltrati,creati e gestiti attraverso la piattaforma Google Suite for Education.

Di conseguenza, lo studente sottoscrive anche le regole di comportamento – la cui infrazione comporterà sanzioni - affinché il servizio possa funzionare nel miglior modo possibile, tenendo presente che cortesia ed educazione, che regolano i rapporti comuni tra le persone,valgono anche in questo contesto.

Di seguito la **Netiquette** indicata nella liberatoria:

1. Poiché il servizio è uno dei mezzi di comunicazione tra Docenti e lo Studente, dovrai accedere alla piattaforma con frequenza quotidiana;
2. se utilizzi un PC non esclusivamente tuo userai sempre il software Google Chrome o Firefox in modalità NAVIGAZIONE IN INCOGNITO;
3. in POSTA e in GRUPPI invierai messaggi brevi che descrivono in modo chiaro di cosa stai parlando;indicherai sempre chiaramente l'oggetto in modo tale che il destinatario possa immediatamente individuare l'argomento della email ricevuta;
4. non inviare mai lettere o comunicazioni a catena che causano un inutile aumento del traffico in rete;
5. non utilizzare la piattaforma in modo da danneggiare, molestare o insultare altre persone;
6. non creare e non trasmettere immagini, dati o materiali offensivi, osceni o indecenti;

7. non creare e non trasmettere materiale offensivo per altre persone o enti;
8. non creare e non trasmettere materiale commerciale o pubblicitario se o espressamente richiesto;
9. quando condividi documenti non interferire, danneggiare o distruggere il lavoro dei tuoi docenti o dei tuoi compagni;
10. non curiosare nei file e non violare la riservatezza degli altri studenti;
11. usa il computer e la piattaforma Google Workspace in modo da mostrare considerazione e rispetto per compagni e insegnanti.

L'Istituto, dunque, in relazione alle direttive e alle indicazioni, si impegna alle seguenti azioni per la cybersecurity:

- Mantenere separate le reti didattica e segreteria;
- aggiornare periodicamente software e sistema operativo;
- definire la programmazione di backup periodici;
- garantire formazione adeguata allo staff, incluso il corpo docenti;
- testare regolarmente le possibili vulnerabilità;
- preparare piani di azione in risposta ai problemi più seri;
- predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo;
- impostare il browser per eliminare dei cookies alla chiusura;
- definire una policy sulla password: le password devono essere forti;
- minimizzare i privilegi amministrativi;
- sviluppare il regolamento sull'uso delle tecnologie a scuola (policy di uso accettabile).

Si allegano, inoltre, anche le 'Linee Guida in tema di privacy e sicurezza informatica' approvate dal nostro istituto all'interno del Regolamento per lo svolgimento delle sedute collegiali in modalità telematica.

Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli

più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

Il nostro istituto dispone dei seguenti strumenti di comunicazione:

a) Sito web della scuola

La scuola è dotata di sito internet https://www.icscalea.edu.it/

Il sito si configura come un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali e avvisi di carattere generale.

L'inserimentodeicontenutièpossibilesoloagliaddettidelpersonalediSegreteria,perquantoriguarda i dati di tipo economico-amministrativo; alcuni docenti gestiscono le pagine descrittive dell'Istituto e delle attività che vi si svolgono.

Il personale che è in possesso delle credenziali per la gestione dei contenuti sul portale si assumerà la responsabilità editoriale di garantire che il contenuto inserito sia accurato e appropriato, anche e soprattutto ai fini del rispetto del Codice dell'Amministrazione Digitale (CAD).

b) Registro elettronico

Fra gli strumenti di comunicazione interna si annovera il registro elettronico, con tutte le sue funzionalità. Le famiglie, così, possono visualizzare molte informazioni utili, interagendo con la scuola, su:

- andamento scolastico;
- risultati scolastici (voti, documenti di valutazione);
- eventi;
- comunicazioni varie.

c) Google Workspace (vd. supra).

d) Strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne

In riferimento all'uso degli strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne, come avviene generalmente fra i docenti mediante ad esempio l'uso di gruppi Whatsapp o Telegram, è importante ricordare quello che si può definire "diritto alla disconnessione". L'art. 22 (Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola) del CCNL 2016/2018, infatti, fa riferimento ai criteri generali per l'utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio, al fine di una maggiore conciliazione fra vita lavorativa e vita familiare.

Lo stato emergenziale vissuto nell'a.s. 2019/2020 ha favorito la comunicazione informale fra colleghi e docenti, nonché eccezionalmente anche un primo raggiungimento degli allievi e delle famiglie, allo scopo di attivare in tempi brevi la didattica a distanza.

È importante sottolineare, però,che non esiste una vera e propria regolamentazione per la circolazione di informazioni e di comunicazione interne tramite gli strumenti online e, per tale ragione è fondamentale, a partire dal buon senso e da una riflessione sulle peculiarità del mezzo, predisporre comunque delle regole condivise sull'uso delle stesse, come quelle indicate di seguito:

- Mettere in chiaro fin dall'inizio, comprendere e rispettare sempre le finalità del gruppo, scrivendo e pubblicando solo contenuti pertinenti a tali finalità;
- usare sempre un linguaggio adeguato e il più possibile chiaro e preciso (come già sottolineato la comunicazione online si presta spesso a non pochi fraintendimenti);
- evitare di affrontare in chat argomenti troppo complessi e controversi (la comunicazione online in una chat di gruppo non è adatta per la gestione di problematiche di questo tipo, che certamente è più opportuno affrontare in presenza o in un Consiglio di classe);
- evitare discussioni di questioni che coinvolgono due o pochi interlocutori, onde evitare di annoiare e disturbare gli altri componenti del gruppo;
- non condividere file multimediali troppo pesanti;
- evitare il più possibile di condividere foto di studenti in chat;
- indirizzare solo domande precise e chiare, a cui si possano dare risposte altrettanto brevi e precise;
- evitare messaggi troppo spezzettati, cercando il più possibile di essere brevi ed esaustivi allo stesso tempo.

Si ricorda, inoltre, quando si usano invece chat formali, create ad esempio dal Dirigente scolastico per veicolare messaggi, informazioni e aggiornamenti relativi all'attività scolastica, la regolamentazione è prevista dalla contrattazione di Istituto.

La contrattazione di istituto al titolo VIII "CRITERI GENERALI PER L'UTILIZZO DI STRUMENTAZIONI TECNOLOGICHE DI LAVORO IN ORARIO DIVERSO DA QUELLO DI SERVIZIO, AL FINE DI UNA MAGGIORE CONCILIAZIONE TRA VITA LAVORATIVA E VITA FAMILIARE (DIRITTO ALLA DISCONNESSIONE).(art.22 comma 4 lettera C8 CCNL Scuola 2018)" stabilisce che:

Art. 34 Tipologia e modalità di comunicazione.

Gli strumenti elettronici per la comunicazione si distinguono in strumenti sincroni e asincroni. I primi, a differenza dei secondi, richiedono che entrambi i terminali della comunicazione (trasmittente e ricevente) siano connessi perché si abbia comunicazione.

La comunicazione telefonica tradizionale richiede la connessione tra chi trasmette e chi riceve.

La messaggistica (whatsapp, mail, messanger) può avvenire anche se una delle due parti non è connessa, in questo caso chi riceve decide tempi e modalità di consultazione dei messaggi ricevuti.

Art. 35 Modalità e tempi di convocazione e delle comunicazioni ufficiali.

Le convocazioni ufficiali degli organi collegiali, degli incontri scuola famiglia, degli organi tecnici devono avvenire con comunicazione scritta, pubblicata nel sito web della scuola, con i giorni di preavviso previsti per legge o dai regolamenti.

Le comunicazioni pubblicate nel sito web devono essere consultate e lette dai docenti e dal personale ATA.

Le richieste di adempimenti e le convocazioni fissate per il giorno della ripresa delle attività didattiche, dopo un periodo di vacanza, non possono essere pubblicate il giorno precedente il periodo festivo stesso.

Art. 36 Diritto alla disconnessione.

Questo strumento contrattuale vuole tutelare la conciliazione tra vita lavorativa e vita familiare, così si eliminano l'invasività del datore di lavoro e l'obbligo per il lavoratore di rimanere connessi 24 ore su 24 e 7 giorni su 7: la contrattazione integrativa stabilisce che il dirigente scolastico e la scuola potranno fornire informazioni telefoniche e messaggistiche ai dipendenti dalle 08.00 alle 14.00 e dalle 15.30 alle 18.00.

Art. 37 Modalità e tempi di utilizzo delle comunicazioni sincrone (telefoniche).

I lavoratori non possono essere contattati telefonicamente per problematiche riguardanti la prestazione lavorativa durante il periodo di sospensione delle attività didattiche e nei periodi festivi.

I collaboratori del dirigente scolastico, le funzioni strumentali i responsabili di plesso, i docenti che hanno compiti organizzativi, in caso d'urgenza, possono essere contattati anche fuori dai suddetti limiti temporali.

Nei limiti dell'orario di funzionamento degli uffici di segreteria e di presidenza è possibile contattare i lavoratori durante il periodo di sospensione delle attività didattiche per comunicazioni connesse al proprio stato giuridico o economico.

Per ragioni di sicurezza ed emergenza i suddetti limiti sono superati al fine di evitare o prevenire situazioni di pericolo.

Art. 38 Modalità e tempi di utilizzo delle comunicazioni asincrone (messaggistica).

La comunicazione tramite i "canali sociali" non richiedono la connessione contestuale e contemporanea dei lavoratori. In questo caso è possibile inviare comunicazioni anche in periodi non lavorativi poiché è garantita la piena libertà del lavoratore di scegliere i tempi di lettura e di replica. A tal fine, trattandosi di trasmissione di messaggi, che non richiedono la connessione contemporanea, i lavoratori (tra questi è incluso anche il dirigente scolastico) possono decidere i tempi di trasmissione dei messaggi, fatto salvo il diritto di chi riceve di leggere e replicare nei tempi desiderati.

In ogni caso le comunicazioni a mezzo dei canali sociali informatici con gli utenti e con i colleghi devono essere finalizzate ad informazioni di servizio e alle interazioni necessarie per lo svolgimento della funzione di educazione, di istruzione e di orientamento.

3.3 - BYOD

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

Strumentazione personale

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.

Per tale ragione, l'Istituto si impegnerà ad attivare, in contesti di totale sicurezza, l'utilizzo dei dispositivi in classe, a seconda dei vari usi, anche in considerazione dei già citati dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

La presente ePolicy contiene indicazioni e integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, prevedendo misure per prevenire tipologie di rischio (non solo come quelle più frequenti come il cyberbullismo) e stabilire procedure specifiche per rilevare e gestire le diverse problematiche. Risulta fondamentale, pertanto, per la nostra 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 sia i lati positivi che eventuali criticità nella e per la didattica.

Di seguito è indicato come l'utilizzo della strumentazione personale è regolamentata all'interno del nostro Istituto.

1. *Per la componente studentesca*

- I telefoni cellulari, i tablet e le relative fotocamere e registratori vocali non verranno utilizzati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate dal corpo docente.
- L'insegnante della prima ora ricorda agli alunni di spegnere i cellulari (si rimanda al Regolamento d'Istituto che disciplina le diverse sanzioni per l'uso improprio del dispositivo mobile).
- Alunni con disturbi specifici di apprendimento, previa consultazione con il Consiglio di Classe, concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili e le modalità di custodia degli stessi.
- Giochi e console, tra cui la Sony Playstation, Microsoft Xbox e similari, che possono avere accesso a Internet non filtrato, non sono consentiti nemmeno se custoditi come previsto per gli altri dispositivi. Saranno requisiti dal docente che ravvisa l'infrazione, depositati in dirigenza e consegnati al genitore/tutore convocato, che sarà contestualmente informato dell'eventuale sanzione disciplinare comminata al trasgressore.
- Nel caso in cui debbano comunicare con la famiglia durante l'orario scolastico, alunne e alunni possono usare gratuitamente la linea fissa della scuola rivolgendosi a un operatore; allo stesso modo le famiglie devono chiamare il centralino della scuola se hanno assoluta necessità di parlare con i propri figli. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.
- L'invio di materiali abusivi, offensivi o inappropriati è vietato, anche se avviene all'interno di cerchie o gruppi di discussione privati.

Per il personale docente/ata

- Il personale preferirà, quando ciò è possibile, l'impiego della strumentazione fornita dalla scuola rispetto a quella personale (portatili, pc fissi, ...).

- le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali.

- Telefoni cellulari, tablet, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate.

- La password di accesso alla rete va custodita con cura e per nessuna ragione deve essere divulgata a chi non ha titolo per utilizzarla (studenti, genitori, operatori esterni).

- Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (chiavette usb, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.

Durante l'attività didattica è opportuno che ogni insegnante:

- Dia chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforma studenti, ecc.), condividendo con gli studenti la netiquette e indicandone le regole;

- si assuma la responsabilità di segnalare prontamente eventuali malfunzionamenti o danneggiamenti al tecnico informatico;

- non salvi sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili e proponga agli alunni attività di ricerca di informazioni in rete fornendo opportunamente loro indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento.

Utilizzo del laboratorio di informatica e della postazioni di lavoro

La scuola è già dotata di un regolamento di fruizione e di utilizzo del laboratorio di informatica che si configura come allegato alla presente. Tuttavia è utile, in questa Policy, ricordare le disposizioni generali sull'uso dei laboratori:

1. Le apparecchiature presenti nella scuola sono patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.

2. I laboratori informatici e le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.

3. Quando un insegnante, da solo o in classe, usufruisce del laboratorio deve registrare il proprio nome e l'eventuale classe nell'apposito registro delle presenze di laboratorio, indicando il numero della postazione utilizzata. Questo allo scopo di poter risalire alle cause di eventuali inconvenienti o danneggiamenti e per comprovare l'effettivo utilizzo dell'aula.

4. L'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante.

5. Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software.

6. Nei laboratori è vietato utilizzare CD personali o altri dispositivi se non dopo opportuno controllo con sistema di

antivirus aggiornato.

7. All'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il locale in ordine e le macchine spente correttamente

8. In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile del laboratorio.

9. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante.

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

Cap 4 - Segnalazione e gestione dei casi

4.1 - Cosa Segnalare

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. Queste, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola.

Nelle procedure sono indicate le figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso, nonché le modalità di coinvolgimento del Dirigente Scolastico e del Referente per il contrasto al bullismo e al cyberbullismo. 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. 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, per quanto possibile, la rimozione del materiale on-line e il blocco della sua diffusione per mezzo dei 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.

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

- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- docente referente e team per il contrasto del bullismo e cyberbullismo per le segnalazioni.

4.2 - Quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale (ex art. 357 c.p.) 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.

Il Codice Penale Italiano, all'art. 357, definisce il pubblico ufficiale come colui che esercita una "pubblica funzione legislativa, giudiziaria o amministrativa". Questa definizione si estende ai docenti nel momento in cui sono impegnati nell'esercizio delle loro funzioni all'interno degli istituti scolastici.

La Corte di Cassazione, con la sentenza n. 15367/2014, ha ribadito la qualifica di pubblico ufficiale per l'insegnante, estendendo tale riconoscimento non solo alla tenuta delle lezioni, ma anche a tutte le attività connesse. Questo include, ad esempio, gli incontri con i genitori degli allievi.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite da un team di docenti composto da:

1. Dirigente
2. Docente referente,
3. L'animatore digitale (secondo il Piano Nazionale per la Scuola Digitale, abbreviato in PNSD, introdotto dalla Legge 107/2015)
4. Referente bullismo (ex. Legge Italiana Contro il Cyberbullismo, l. 71/2017
5. Altri docenti già impegnati nelle attività di promozione dell'educazione civica.

Le situazioni di pregiudizio presunto o reale possono richiedere il supporto e l'intervento di esperti esterni alla scuola.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due macro - 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.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l'obiettivo di allertare il Dirigente . La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, il Dirigente e i docenti coinvolti procedono alla valutazione del caso (valutare l'invio o meno della relazione agli organi giudiziari preposti) e agiscono tramite percorsi di sensibilizzazione.

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.

In questo caso, l'informazione relativa al sospetto deve essere inoltrata al Referente e al team dei docenti "antibullismo" con l'obiettivo di allertare il Dirigente. La comunicazione dovrebbe avere una forma scritta e riportare tutti i dati e le informazioni in maniera dettagliata e oggettiva. Da qui, si procede alla valutazione approfondita e alla verifica di quanto segnalato, avviando (se appurato la rilevanza penale) la procedura giudiziaria con denuncia all'autorità giudiziaria per attivare un procedimento penale.

Qualora si rilevasse un fatto riconducibile alla fattispecie di reato, l'insegnante - nel ruolo di pubblico ufficiale – non deve procedere con indagini di accertamento ma ha sempre l'obbligo di segnalare l'evento all'autorità giudiziaria. (ex. l. 71/2017). Con autorità competente si intendono:

- Procure Ordinarie: nel caso in cui il minore/i sia la vittima/e e il presunto autore del reato sia maggiorenne,
- Procura Minorile: in caso il presunto autore del reato sia minorenne.

Vi è anche l'obbligatorietà della segnalazione delle situazioni di pregiudizio a carico dei minori: L. 216/1991: per le situazioni di grave rischio l'istituzione scolastica è tenuta alla segnalazione delle medesime. Per pregiudizio si intende una condizione di rischio o grave difficoltà che provocano un danno reale o potenziale alla salute, alla sopravvivenza, allo sviluppo o alla dignità del bambino, nell'ambito di una relazione di responsabilità, fiducia o potere.

La segnalazione come da procedura interna è il primo passo per aiutare un minore che vive una situazione di rischio o di grave difficoltà e va intesa come un momento di condivisione e solidarietà nei confronti del minore. La mancata segnalazione costituisce, infatti, omissione di atti d'ufficio (art.328 C.P.).

Può essere utile, valutando accuratamente ciascuna situazione, attivare colloqui individuali con tutti i minori coinvolti, siano essi vittime, testimoni e/o autori. È importante considerare il possibile coinvolgimento dei genitori e di coloro incaricati della tutela dei minori coinvolti. L'intervento va indirizzato valutando l'eventuale impatto educativo e/o il contesto emotivo senza discriminare tra vittime, testimoni e/o autori.

Prevedere possibili incontri di mediazione tra i minori coinvolti vanno ponderati con la consapevolezza del loro stato emotivo, anche e in base agli elementi raccolti in merito del fatto/episodio avvenuto (elementi che si dovrebbero valutare di caso in caso). Importante è prevedere il coinvolgimento dei genitori sia della vittima che del bullo (ove possibile).

Anche i genitori devono e possono segnalare casi di sospetto o evidenza dei fenomeni, segnalarlo al Dirigente, o al docente coordinatore di classe o referente di istituto oppure direttamente al team antibullismo attraverso apposita procedura che definisce l'istituto (mail ad hoc, tramite gli uffici e postazioni specifiche, etc...).

Gli insegnanti e i genitori, come studenti e studentesse, si possono rivolgere alla Helpline del progetto Generazioni Connesse, al numero gratuito 19696, attraverso la chat disponibile sul sito o tramite chat WhatsApp per ricevere supporto e

consulenza. Per tutti i dettagli, il riferimento è agli allegati con le procedure.

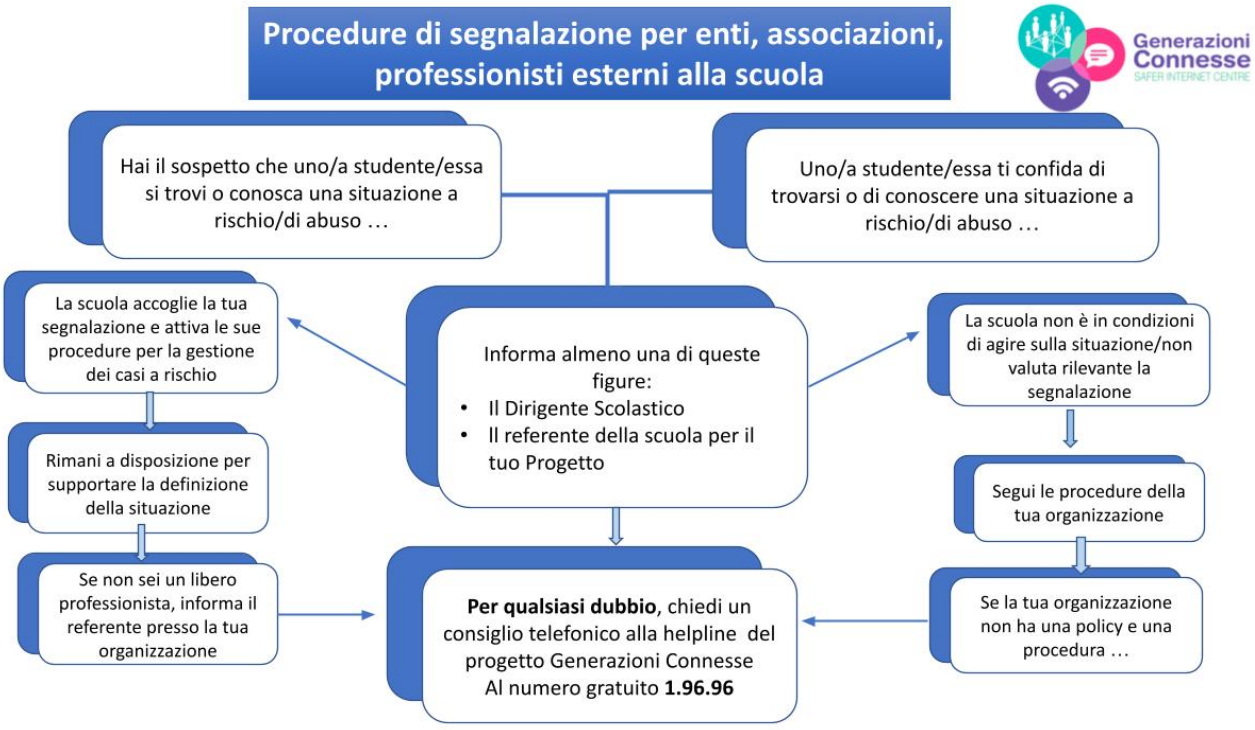
Strumenti a disposizione di studenti/esse

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.

In particolare, sarebbe utile che la scuola attivi un sistema di segnalazione utile anche al monitoraggio dei fenomeni dal quale partire per integrare azioni didattiche preventive e giornate di sensibilizzazione, insieme agli Enti/Servizi presenti sul territorio di riferimento. Importante, altresì, immaginare e programmare percorsi di peer education per la prevenzione e il contrasto degli agiti.

Per ulteriori chiarimenti in merito, si rimanda al Regolamento di disciplina degli studenti e delle studentesse, integrato con la previsione di infrazioni disciplinari legate a comportamenti scorretti assunti durante la DID e relative sanzioni, alle Linee di Orientamento per la prevenzione e il contrasto dei fenomeni di Bullismo e Cyberbullismo del MI (Ministero dell'Istruzione) aggiornate al 2021, al Patto educativo di corresponsabilità e annessa appendice relativa agli impegni che le parti in causa dovranno assumere per l'espletamento efficace della DID e, in ultimo, al Piano scolastico per la Didattica Digitale Integrata, allegato al PTOF.

Procedure



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

Il docente ha evidenza che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Se non è già stato fatto, avvisa il referente per il cyberbullismo (e/o il team antibullismo) che attiva le procedure ("Corso 4" della piattaforma ELISA) e il Dirigente Scolastico.
Ricordare sempre che in base alla legge 71-2017:
A) Se c'è fattispecie di reato va fatta la segnalazione alle forze dell'ordine
B) Se non c'è fattispecie di reato.
Il DS (e/o il team antibullismo):
- informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto) su quanto accade e condividete informazioni e strategie.
- Informa i genitori di ragazzi/e infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy)
- Attiva il consiglio di classe.

A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnala alla Polizia Postale:
a) contenuto; b) modalità di diffusione.
Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).

Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

NELLE CLASSI
Il team antibullismo collabora coi docenti della classe per realizzare l'intervento nella classe:
a seconda della situazione valuta se
- affrontare direttamente l'accaduto o
- sensibilizzare la classe (vedi Corso 4 Piattaforma Elisa)
- trova il modo di supportare la vittima e di responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo

Il docente riceve una segnalazione (da un genitore, un altro studente …) o sospetta che stia accadendo qualcosa a uno/a studente/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Condividi con il referente o al team antibullismo: si attiva il processo di attenzione e valutazione a cura del referente.

Insieme si valuta se è il caso
- di avvisare il consiglio di classe;
- di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.

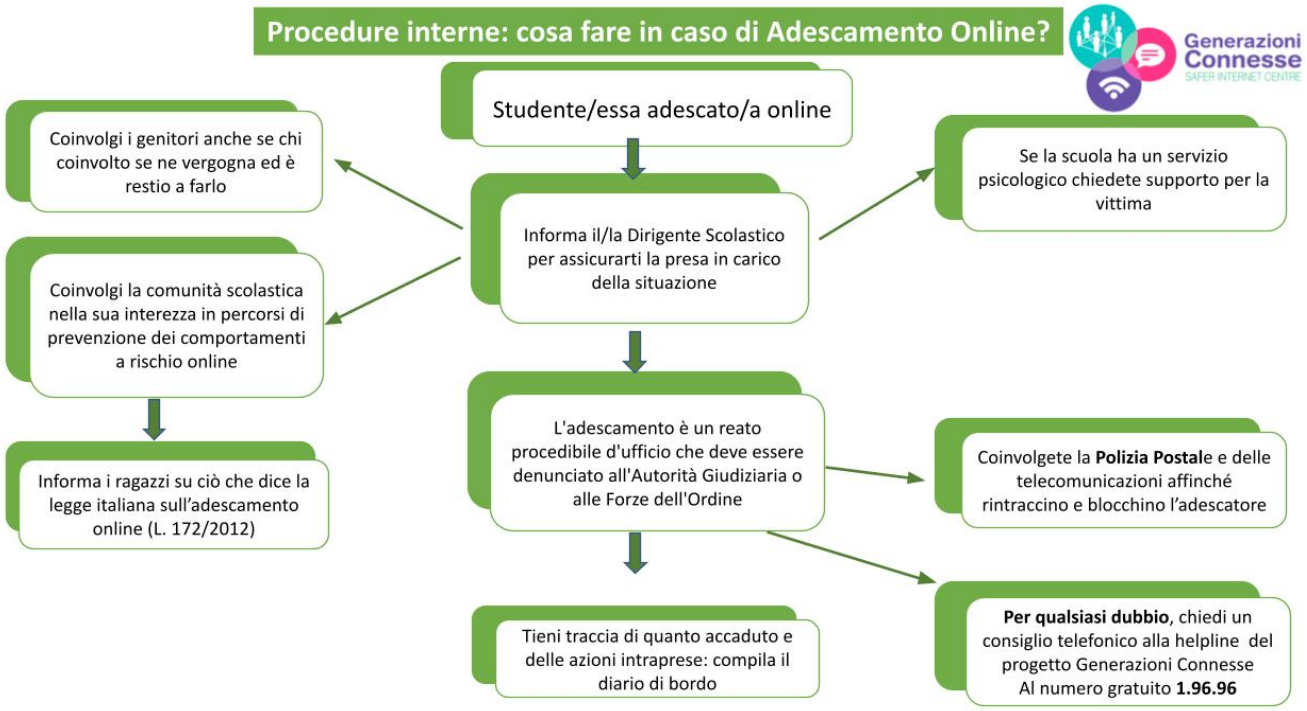
Se emergono evidenze passa allo schema successivo

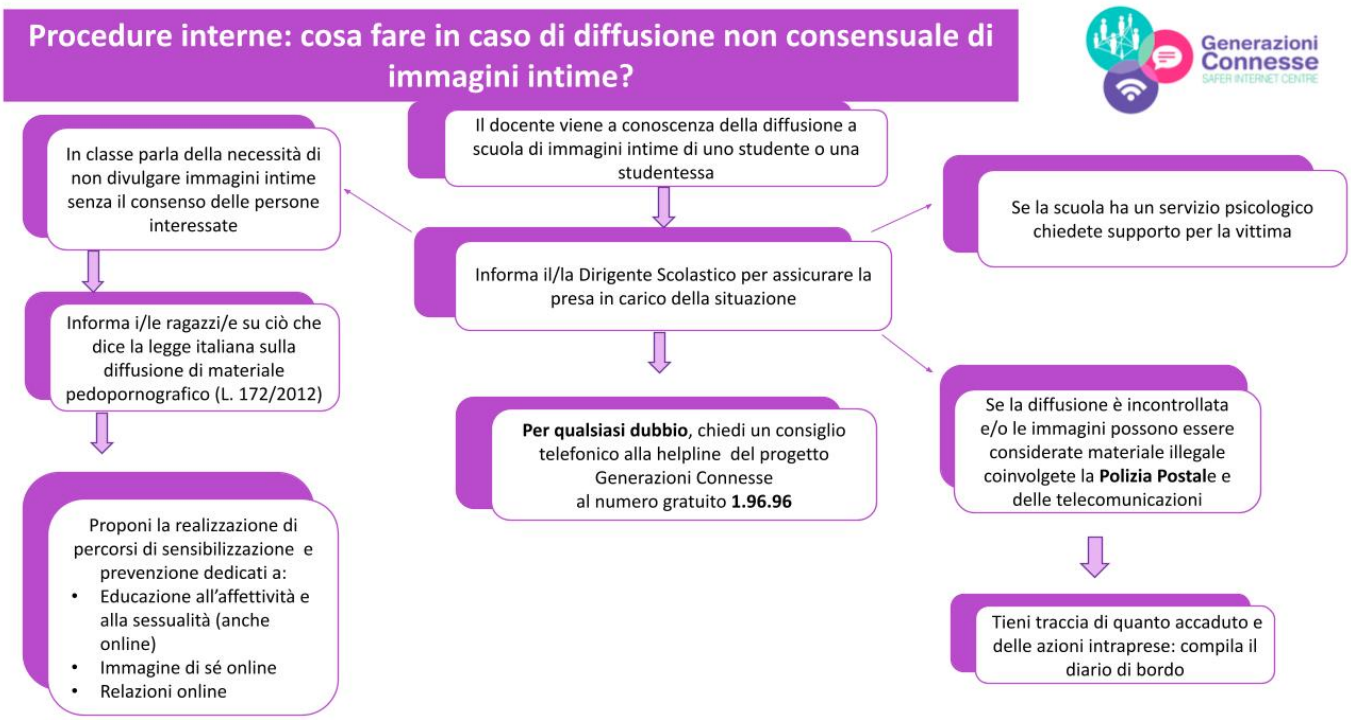
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Ricorda a studenti/esse che possono chiedere in qualsiasi momento una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 o via chat

Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

Scarica le linee di orientamento per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo





La scuola prevede, per le procedure di segnalazione, anche i moduli che Generazioni Connesse ha fornito nel corso della prima adesione (a.s. 2020/2021). Saranno fruibili sul sito della scuola, nella sezione dedicata insieme alle procedure sopra indicate.

Saverio Ordine
15.06.2026
11:43:43
GMT+02:00