

DOCUMENTO DI ePOLICY

A.S. 2021/2022

Direzione didattica Nola 2

“M. Sanseverino”

Via A. Ciccone
80035 – Nola (NA)

Dirigente prof.ssa Giuseppina La Montagna

A cura del team ePolicy

SOMMARIO

Capitolo 1

Scopo dell'ePolicy

Ruoli e responsabilità

Un'informativa per i soggetti esterni

Condivisione e comunicazione dell'ePolicy

Gestione delle infrazioni alla ePolicy

Integrazione dell'ePolicy con Regolamenti esistenti

Monitoraggio e aggiornamento dell'ePolicy

Capitolo 2

Curricolo sulle competenze digitali

Formazione dei docenti

Capitolo 3

Accesso a Internet e filtri per la navigazione

E-mail

Sito web della scuola

Protezione dei dati personali

Laboratori informatici

Capitolo 4

Sensibilizzazione e prevenzione

Cyberbullismo: che cos'è e come prevenirlo

Capitolo 5

Segnalazione e gestione dei casi

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 alunni 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 Istituzione scolastica 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, oltre che 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 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 digita

1.2 - Ruoli e responsabilità

Con questo documento tutta la comunità scolastica è chiamata ad attuare e a promuovere il piano. Ciascuno in base al proprio ruolo e alle proprie responsabilità.

Il Dirigente scolastico

- Garantisce la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- garantisce ai propri docenti una formazione di base sulle tecnologie dell'Informazione e della Comunicazione (ICT) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse;
- garantisce l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on-line;
- informa tempestivamente, qualora venga a conoscenza di atti di cyberbullismo che non si configurino come reato, i genitori dei minori coinvolti (o chi ne esercita la responsabilità genitoriale o i tutori);
- regola il comportamento degli alunni ed impone sanzioni disciplinari in caso di comportamento inadeguato.

Il referente del Cyberbullismo d'Istituto

- Coordina iniziative di prevenzione e contrasto del cyberbullismo messe in atto dalla scuola;
- predispone un documento di rilevazione di incidenti di sicurezza in rete;
- facilita la formazione e la consulenza di tutto il personale.

Animatore digitale e Team dell'innovazione

- Pubblicano il presente documento di e-Safety Policy sul sito della scuola;
- diffondono i contenuti del documento tra docenti e alunni;
- coordina la prenotazione dei laboratori informatici consentendo di tenere traccia di ora e laboratorio utilizzati da ciascuno.

Direttore dei Servizi Generali e Amministrativi

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

Tecnico incaricato per manutenzione della rete e degli apparati

- Può controllare gli accessi ad internet

- è l'unico a poter installare nuovi software;
- limita l'accesso ad alcuni siti;

Genitori

- Contribuiscono, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- incoraggiano l'impiego delle ICT da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga in sicurezza;
- agiscono in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite;
- rispondono per gli episodi commessi dai figli minori a titolo di colpa in educando (articolo 2048 del Codice Civile).
- sono esonerati da responsabilità solo se dimostrano di non aver potuto impedire il fatto. Nei casi più gravi i giudici per l'inadeguatezza dell'educazione impartita ai figli emerge dagli stessi episodi di bullismo, che per le loro modalità esecutive dimostrano maturità ed educazione carenti.

Gli enti educativi esterni e le associazioni

- Osservano le politiche interne sull'uso consapevole della Rete e delle TIC;
- attivano procedure e comportamenti sicuri per la protezione degli alunni e delle alunne durante le attività che vengono svolte all'interno della scuola o in cui sono impegnati gli stessi.

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

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

Tutti gli attori che entrano in relazione educativa con gli alunni e le alunne 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 alunni 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 della nostra Istituzione scolastica in riferimento alle 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 alunni e le alunne.

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).

Ambiti di applicazione, attività e ruoli

Le attività progettuali o di formazione devono essere preventivamente autorizzate dal Dirigente scolastico, con modalità e tempi concordati; a tal proposito, al fine di verificare preventivamente il contenuto da somministrare o dibattere con la scolaresca, i soggetti esterni forniranno un dettagliato programma delle attività con narrazione sintetica della scaletta al fine di essere autorizzato dalla Dirigenza.

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 alunni e le alunne, e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico si faccia a sua volta promotore del documento.

L'E-policy viene condivisa e comunicata al personale, agli alunni e alle alunne, 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 alunni e le alunne 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.

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.

Disciplina degli alunni

- Richiamo verbale;
- sanzioni estemporanee commisurate alla gravità della violazione commessa (assegnazione di attività aggiuntive da svolgere a casa sui temi di Cittadinanza e Costituzione);
- nota informativa ai genitori o tutori mediante registro elettronico;
- convocazione dei genitori o tutori per un colloquio con l'insegnante;

- convocazione dei genitori o tutori per un colloquio con il Dirigente Scolastico;
- denunce di bullismo On-line saranno trattate in conformità con la legge.
-

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 e alcune possono determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli allievi:

- utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di docenza o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiale non idoneo;
- utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- trattamento dei dati personali e dei dati sensibili degli alunni non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- carente istruzione preventiva degli alunni sull'uso corretto e responsabile delle TIC e di internet;
- vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili rischi connessi;

- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.

Il Dirigente scolastico può disporre il controllo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola; può disporre la cancellazione di materiali non adeguati o non autorizzati dal sistema informatico della scuola, e se necessario ne conserva una copia per eventuali approfondimenti successivi.

Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio dei procedimenti che possono avere carattere organizzativo-gestionale, disciplinare, amministrativo, penale, a seconda del tipo e della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

Disciplina dei genitori

In considerazione dell'età degli alunni e della loro dipendenza dagli adulti, anche talune condizioni e condotte dei genitori medesimi possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli allievi a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico.

Gli atteggiamenti da parte della famiglia da evitare sono:

- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non corre rischi;
- una postazione del computer in una stanza o in una postazione non visibile e controllabile dall'adulto;
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'uso di cellulare o smartphone;
- un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei a minori;
- un utilizzo di cellulari e smartphone in comune con gli adulti che possono conservare in memoria indirizzi di siti o contenuti non idonei a minori.

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per altri (colpa in educando e in vigilando).

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

Il documento ePolicy è parte integrante del nostro PTOF, del regolamento dell'Istituto

dell'Istituzione scolastica e del Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

Il monitoraggio e la revisione della e-Policy sarà svolta annualmente e /o qualora si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno dell'Istituto.

L'aggiornamento del documento di e-Policy sarà curato dal docente Referente di Istituto per la prevenzione e il contrasto del bullismo e cyberbullismo, in qualità di coordinatore del gruppo di lavoro del presente documento e con la partecipazione dell'Animatore digitale.

CAPITOLO 2 - FORMAZIONE E CURRICOLO

2.1. Curricolo sulle competenze digitali per gli alunni

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 alunni verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale.

Le finalità formative delle TIC possono essere sintetizzate nei seguenti punti:

- Favorire la conoscenza dello strumento pc e/o tablet a scopo didattico
- Sostenere l'alfabetizzazione informatica
- Favorire la trasversalità delle discipline
- Facilitare il processo di apprendimento
- Favorire il processo di inclusione
- Fornire nuovi strumenti a supporto dell'attività didattica
- Promuovere situazioni collaborative di lavoro e di studio
- Sviluppare creatività e capacità di lavorare in gruppo
- Promuovere azioni di cittadinanza attiva
- Utilizzare in modo critico, consapevole e collaborativo la tecnologia.

Competenze digitali declinate secondo le cinque aree del quadro di riferimento

DIGCOM (Quadro comune di riferimento europeo per le competenze digitali):

1. INFORMAZIONE: identificare, localizzare, recuperare, conservare,

organizzare e analizzare

2. **COMUNICAZIONE:** comunicare in ambienti digitali, condividere risorse attraverso strumenti on-line, collegarsi con gli altri e collaborare attraverso strumenti digitali, interagire e partecipare alle comunità e alle reti;
3. **CREAZIONE DI CONTENUTI:** creare e modificare nuovi contenuti (da elaborazione testi a immagini e video); integrare e rielaborare le conoscenze ed i contenuti; produrre espressioni creative, contenuti media e programmare; conoscere e applicare i diritti di proprietà intellettuale e le licenze;
4. **SICUREZZA:** protezione personale, protezione dei dati, protezione dell'identità digitale, misure di sicurezza, uso sicuro e sostenibile;
5. **PROBLEM-SOLVING:** identificare i bisogni e le risorse digitali, valutare appropriati strumenti digitali secondo lo scopo o necessità, risolvere problemi concettuali attraverso i mezzi digitali, utilizzare creativamente le tecnologie, risolvere problemi tecnici, aggiornare la propria competenza e quella altrui.

COMPETENZA DIGITALE

TRAGUARDI PER LO SVILUPPO DELLE COMPETENZE

Al termine della Scuola dell'Infanzia

- Comunicare ed esprimersi con una pluralità di linguaggi, avvalendosi anche della strumentazione tecnologica
- Orientarsi, con la guida dell'insegnante, nel mondo delle tecnologie

Al termine della Scuola Primaria

- Si orienta tra i diversi mezzi di comunicazione ed è in grado di farne un uso adeguato a seconda delle diverse situazioni.
- Produce semplici modelli o rappresentazioni grafiche del proprio operato utilizzando elementi del disegno tecnico o strumenti multimediali.
- Inizia a riconoscere in modo critico le caratteristiche, le funzioni e i limiti della tecnologia attuale.
-

COMPETENZE SPECIFICHE

Scuola dell'Infanzia

- Utilizzare strumenti informatici in situazioni di gioco e/o come supporto didattico
- Utilizzare le TIC per produrre, rivedere e documentare il proprio lavoro

Scuola Primaria

Classe terza

- Utilizzare il computer in un contesto applicativo
- Utilizzare strumenti informatici e di comunicazione in situazioni significative di gioco e come supporto didattico
- Utilizzare le tic come strumento per produrre, rivedere e documentare il proprio lavoro

Classe quinta

- Recuperare e analizzare informazioni da fonti diverse
- Utilizzare le TIC in modo creativo e funzionale allo studio, alla collaborazione e alla comunicazione

ABILITA'

Scuola dell'Infanzia

- Utilizzare, con la supervisione dell'insegnante, alcune TIC per documentare un'esperienza vissuta, per fare ricerca, per conoscere

Scuola Primaria

Classe terza

- Usare in modo guidato i giochi didattici multimediali
- Usare semplici programmi grafici per disegnare e colorare (paint)
- Sapersi orientare tra gli elementi principali del computer e le loro funzioni
- Saper utilizzare gli elementi per immettere dati, stampare e salvare un documento

Classe quinta

- Saper utilizzare dispositivi per memorizzare i dati
- Archiviare documenti secondo un criterio stabilito creando cartelle
- Saper usare programmi didattici presenti sul PC
- Saper svolgere giochi didattici multimediali adeguati alle proprie competenze Saper trovare informazioni su internet a scopi didattici
- Costruire ed elaborare tabelle di dati con la supervisione dell'insegnante
- Formattare testi scritti inserendo elementi grafici.
- Utilizzare la rete per inviare e-mail legate ad attività didattiche attraverso l'uso di account della scuola o autorizzati e visionati dai genitori
- Creare artefatti digitali utilizzando semplici applicativi

- Utilizzare la rete in modo consapevole attuando comportamenti preventivi.

CONOSCENZE

Scuola dell'Infanzia

- Alcune strumentazioni tecnologiche e loro utilizzo.

Scuola Primaria

Classe terza

- Giochi didattici multimediali
- Principi d'uso dei più noti programmi grafici per disegnare e colorare
- Principali parti e funzioni del computer
- Funzionalità di programmi di videoscrittura con inserimento di tabelle e immagini

Classe quinta

- Funzioni principali dei software più conosciuti (word, excel, power point o simili)
- Fondamentali forme di utilizzo della rete per la ricerca di informazioni.
- Forme di comunicazione attraverso la rete.
- Semplici applicativi per la collaborazione e la produzione e condivisione di informazioni e conoscenze.
- Principali rischi dell'utilizzo della rete con pc e telefonini.

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 alunni modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

Il Collegio docenti riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola, sia quelle liberamente scelte dai docenti (anche online) purché restino coerenti con il piano di formazione, come meglio indicato nel PTOF.

L'attenzione all'uso delle TIC nella didattica rende gli apprendimenti più motivanti, coinvolgenti ed inclusivi, con una funzione di guida da parte del docente; inoltre, permette di sviluppare capacità che sono sempre più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza ed il confronto fra pari in modalità asincrona.

La competenza digitale -oggi- è imprescindibile sia per i docenti sia per gli e permette di integrare la didattica con strumenti che la diversificano, la rendono innovativa ed in grado di venire incontro ai nuovi stili di apprendimento.

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. I momenti di formazione ed aggiornamento sono dunque formulati secondo un'analisi del fabbisogno formativo del corpo docente sull'utilizzo ed integrazione delle TIC nella didattica.

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.

Gli alunni devono attenersi a quanto previsto dai Regolamenti scolastici e dalle Circolari interne emanate dal Dirigente scolastico, sulla base delle note ministeriali sull'utilizzo consapevole delle tecnologie digitali all'interno del contesto scolastico.

I genitori, nell'azione di corresponsabilità didattico-educativa, rappresentano un punto di forza per l'implementazione dei rapporti "scuola-famiglia", quale garanzia e rispetto degli impegni, di natura anche pedagogica, sottoscritti e condivisi nello stesso Patto di corresponsabilità.

CAPITOLO 3 - GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA E NELLA SCUOLA

3.1 - Accesso a Internet e filtri per la navigazione

La nostra Istituzione scolastica dispone dell'accesso alla rete *wi-fi* nel plesso Cicconesi. La rete è dotata di un *firewall* per la prevenzione dagli accessi dall'esterno.

3.2 - E-mail

Tutti i docenti dell'istituto possiedono una e-mail della scuola del tipo: cognome.nome@cdnolasanseverino.edu.it. Gli alunni, per l'utilizzo delle attività didattiche in DaD sono dotati di un indirizzo di posta elettronica della scuola del tipo: cognome.nome@cdnolasanseverino.edu.it

3.3 - Sito web della scuola

Il sito *web* della scuola, <https://www.cdnolasanseverino.edu.it/>, è gestito dall'animatore digitale e da un tecnico che si adoperano affinché il sito sia sicuro e accessibile; hanno cura di effettuare sia aggiornamenti e backup periodici che intervenire in caso di emergenza.

3.4 - Protezione dei dati personali

Ogni docente è responsabile del proprio *username* e della propria *password* di accesso al registro elettronico. In caso di smarrimento o dimenticanza i docenti devono rivolgersi alla segreteria e far presente il problema. A tutto il personale, docente e non docente, è stato raccomandato di non salvare le password nei browser se gli strumenti vengono utilizzati da più persone e di effettuare sempre il logout dai siti a cui si accede con login e dalle caselle di posta personali. In ogni caso è consigliata la navigazione in modalità incognito del browser sulle periferiche della scuola (PC, notebook, tablet, ecc.).

Si invitano altresì i docenti ad una custodia responsabile di tutte le credenziali di accesso con password segrete, alfanumeriche e sicure, cambiate almeno ogni tre mesi.

3.5 - Laboratori informatici

L'Istituto è dotato di laboratori informatici, nei quali è presente una rete LAN cablata che utilizza le stesse protezioni firewall e regole di filtraggio della rete wi-fi.

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 ma è altrettanto importante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano

La nostra Istituzione scolastica intende intervenire attraverso la sensibilizzazione e la prevenzione.

Sensibilizzazione

A partire dalle classi quinte della scuola primaria si punta a informare ma soprattutto ad educare alla consapevolezza e alla riflessione sulle seguenti tematiche:

- Uso o abuso di internet
- Quanto sono dipendente dallo smartphone, che uso ne faccio, per quante ore nell'arco della giornata, riesco a darmi delle regole?
- Come la rete ha modificato il mio modo di comunicare e di pormi in relazione con l'altro; i gruppi whatsapp, la messaggistica sostituiscono il linguaggio verbale e non verbale?
- Quanto sono consapevole dei pericoli della rete, cosa penso di sapere, come penso di evitarli ?

Prevenzione

Oltre a promuovere le competenze previste dal curricolo digitale un accento particolare viene dato:

- alla conoscenza dell'importanza di tutelare la propria privacy e quella degli altri (dati sensibili, password, foto, video) e dell'implicazioni legali in caso di trasgressione;
- alla conoscenza delle regole o norme etiche da tenere in mente quando si naviga in rete, quando si pubblica e/o si condivide un contenuto;
- alla riflessione di come sia possibile dietro uno schermo, protetti dall'anonimato infrangere con facilità tali norme, essere vittime o artefici di azioni lesive e offensive della propria e altrui persona.

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 alunni delle classi quinte 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, soprattutto, 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).

Gli atti di cyberbullismo possono essere suddivisi in due gruppi:

diretto: il bullo utilizza strumenti di messaggistica istantanea come SMS o MMS, che hanno un effetto immediato sulla vittima poiché diretti esclusivamente alla persona;

indiretto: il bullo fa uso di spazi pubblici della Rete, come Social network, blog o forum, per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima, anche dal punto di vista

psicologico.

Indicatori di segnali che può manifestare una potenziale vittima di cyberbullismo sono:

- nervosismo alla ricezione di un messaggio o una notifica;
- disagio nell'andare a scuola o fingere di essere malato (ha spesso mal di stomaco o mal di testa);
- cambiamento del comportamento e degli atteggiamenti in modo repentino;
- ritrosia nel dare informazioni su ciò che fa online;
- mostrare rabbia o depressione soprattutto dopo essere stati online,
- utilizzare sempre meno PC e telefono (arrivando ad evitarli);
- perdere interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;
- il rendimento scolastico peggiora.

Finalità condivisa tra scuola e famiglia è intervenire preventivamente ed efficacemente, al fine di evitare, arginare ed eliminare possibili manifestazioni di comportamenti antisociali.

Valutare i comportamenti che sfociano in disagio sociale è precursore di un lavoro in rete, con la possibilità di coinvolgere anche un servizio specialistico socio-sanitario (Psicologo della scuola, Consultorio familiare, Servizi di Neuropsichiatria, etc.), quale supporto e/o forme di mediazione.

Le tipologie di cyberbullismo maggiormente considerate sono:

- Hate speech (il fenomeno dell'incitamento all'odio, all'intolleranza verso un gruppo o una persona).
- Dipendenza da internet e dal gioco online (i comportamenti patologici/dipendenze).
- Sexting (scambio di contenuti mediali sessualmente espliciti).
- Il grooming o adescamento online (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).
- Denigration (diffusione di pettegolezzi, insulti, voci lesivi della dignità della persona).
- Body shaming (prendere in giro per l'aspetto fisico)

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 alunno/a possa essere vittima o responsabile di una situazione di cyberbullismo, 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.

Vengono individuate:

- le figure preposte all'accoglienza della segnalazione sono i docenti delle classi che provvederanno 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, 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 agli alunni, alle famiglie e a tutti coloro che vivono la scuola.

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

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.

La Dirigente scolastica

Il team

Delibera Collegio dei Docenti epolicy n° 45 del 16/12/2021
Delibera Collegio dei Docenti curricolo digitale n°44 del 16/12/2021

Delibera Consiglio d'Istituto epolicy e curricolo digitale n° 67 del 17/12/2021