



ISTITUTO COMPRENSIVO - MONTEMILETTO
Prot. 0002433 del 10/03/2025
II (Uscita)

Documento di ePolicy I.C. MONTEMILETTO

VIA F. DI BENEDETTO - 83038 - MONTEMILETTO
Avellino (AV) - Campania
Data di approvazione: 07/02/2025 - 21:36

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

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.

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse. Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente). In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti. L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali. Nello specifico: l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo; le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico; le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio; le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

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 pedagogo, 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.

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.

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, il regolamento della privacy e il regolamento BYOD sono redatti in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto. Il documento di E-policy dialoga e si armonizza con gli altri regolamenti vigenti nell'Istituto, integrandosi pienamente con gli obiettivi enunciati nel PTOF, con il Regolamento di Istituto, con il Patto educativo di corresponsabilità controfirmato da Scuola, genitori e studenti all'atto dell'iscrizione.

1.4 Condivisione e comunicazione dell'ePolicy

Il paragrafo dettaglia i seguenti aspetti:

1. il curriculum 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 viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/le studenti/esse) si faccia a sua volta promotore del documento. L'E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso: la pubblicazione del documento sul sito istituzionale della scuola; il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico; Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto.

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 del 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

Azioni da svolgere nei prossimi 3 anni:

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

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

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

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](#)

Con il Documento di e-policy - l'IC Montemiletto vuole tentare di migliorare l'approccio al digitale nonché le modalità di accesso all'informazione. La Rete rappresenta per i più giovani una indubbia fonte di opportunità e stimoli di natura cognitiva, comunicativa e relazionale, d'altro canto un suo incauto utilizzo potrebbe tramutarla in una pericolosa fonte di dipendenza ed esporre a situazioni di vulnerabilità. Irritati dal Cyberspazio, i giovani imboccano talvolta chine pericolose, esasperando e distortendo sentimenti e relazioni: il bullismo, dilagante e devastante, assume oggi le forme subdole e pericolose del Cyberbullismo. In simili frangenti, la Scuola, luogo di formazione, inclusione e accoglienza, ha il dovere di mediare il rapporto tra gli adolescenti e le nuove tecnologie digitali, promuovendone un uso sicuro, consapevole ed efficace. Negli ultimi anni, in particolare, il Ministero dell'Istruzione dell'Università e della Ricerca ha investito molte energie nella promozione del cosiddetto Better Internet for Kids, attraverso molteplici iniziative sorte nell'ambito del PNSD e delle Linee di Orientamento per Azioni di prevenzione e Contrasto al Bullismo e al Cyberbullismo del 2018, diretta emanazione della L. 71/2017 e della recente integrazione contemplata nella L. 70/2024. Tali iniziative hanno trovato il loro coronamento nel progetto Generazioni Connesse, iniziativa sostenuta dalla Commissione Europea e coordinata dal MIUR, realizzata in partenariato con le principali Agenzie nazionali sensibili al tema della sicurezza in Rete: Polizia Postale e delle Comunicazioni, Autorità Garante per l'Infanzia e l'Adolescenza, Save the Children Italia Onlus SOS, Il Telefono Azzurro, Cooperativa EDI (Educazione ai Diritti dell'Infanzia) Movimento Difesa del Cittadino, Agenzia Dire. Il nostro IC, convinto dell'opportunità di integrare le nuove tecnologie nella didattica, è sensibile al benessere psico-fisico dei propri studenti, e si impegna quotidianamente nella promozione di valori e competenze finalizzate all'acquisizione di una cittadinanza digitale consapevole. Attraverso mirati interventi formativi, informativi e partecipativi, in sinergia con Enti territoriali e Agenzie nazionali, l'Istituto intende orientare studentesse e studenti ad un uso responsabile della Rete, fornendo loro le giuste chiavi di lettura per la corretta gestione di relazioni digitali in "agorà" oggettivamente non protette. In particolare, l'adesione al progetto Generazioni Connesse risponde proprio all'esigenza di sostenere studenti, ma anche famiglie e operatori scolastici sui temi della e-Safety mediante nuovi e più efficaci strumenti di contrasto. Rientra in questa prospettiva la redazione della E-Policy, documento programmatico finalizzato a promuovere una coscienza digitale in quanti, da diverse angolature, sono coinvolti nel processo educativo.

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.

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

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

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò sta già accadendo attraverso la progettazione e implementazione di un curriculum digitale d'Istituto, realizzato nell'a.s. 2023-24 ed ampliato nell'a.s. 2024-25.

Al fine di promuovere l'acquisizione delle Digital skills, il nostro Istituto, impegnato da tempo nella realizzazione di azioni coerenti con il PNSD, ha ampliato e integrato la propria offerta formativa con specifici rimandi al tema, pianificando interventi che integrano la dimensione tecnologica, afferente l'acquisizione di saperi di base, con quella cognitiva, legata all'acquisizione e al trattamento dell'informazione, e quella etica, mirante a promuovere un'interazione sociale corretta e responsabile. Già da diversi anni, infatti, vengono attuati percorsi integrati nelle discipline curriculari, di alfabetizzazione digitale ed educazione all'uso consapevole di Internet e dei Social Network; inoltre, in ottemperanza alla L. 71/2017 - Disposizioni a tutela dei minori per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo -rimodulata e consolidata dalla recente L. 70/2024, realizza progetti volti all'educazione alla legalità e alla prevenzione delle nuove e pericolose forme di prevaricazione che hanno per teatro la Rete.

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 curriculum di educazione alla Cittadinanza Digitale previsto dalla L. 92/2019. Il curriculum prende forma attorno all'ePolicy e le attività didattiche sono legate al documento ed alle scelte dell'Istituto al suo interno.

Nel curriculum 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.

La scuola di oggi si confronta con scenari molto più complessi rispetto a pochi anni fa; non si può prescindere ormai dall'ampia diffusione della tecnologia e dei dispositivi digitali, e proprio per questo motivo non si può rinunciare a diffondere "un'educazione digitale" che rilanci il ruolo attivo e responsabile degli utenti e sviluppi attenzione e consapevolezza relativamente ai possibili pericoli presenti in rete. Per i docenti, impegnati in questa rivoluzione tecnologica, si tratta di sperimentare una didattica integrata e innovativa che riconosca il ruolo degli strumenti digitali, padroneggi buone prassi educative, valorizzi i codici delle diverse forme di intelligenza e favorisca l'uso consapevole della tecnologia, anche per quanto concerne l'aspetto dell'inclusione di ciascun alunno.

La scuola deve riconoscere la competenza digitale come un elemento importante nella progettazione di esperienze di apprendimento nelle quali l'alunno possa divenire consapevole del proprio ruolo di "cittadino digitale, di attore proattivo nella società locale, nazionale e globale".

La scuola assume con il digitale una dimensione ampliata "L'aula, attraverso la rete, si apre al mondo".

È da sottolineare come l'apprendimento-insegnamento digitale non sia qualcosa da aggiungere ai curricula d'Istituto. La progettazione didattica della scuola si orienta ad una completa integrazione della tecnologia nel processo di apprendimento perché "la scuola digitale non è un'altra scuola" (dal Piano Nazionale Scuola Digitale).

Nel nostro Istituto Comprensivo si è fortemente percepita la necessità di aggiornamento, in alcuni casi di "alfabetizzazione" digitale, durante l'emergenza nata a seguito del COVID-19 con la conseguente attuazione della DAD - Didattica a Distanza.

Poiché i nostri docenti interagiscono ogni giorno con "nativi digitali" risulta necessario che tutto il corpo docente sia adeguatamente formato a questa forma di comunicazione così come risulta necessario formalizzare nel curriculum digitale i contenuti e le modalità operative che i docenti devono applicare. I nostri alunni sono "nativi digitali", essere "nativo digitale" significa nascere in una società permeata di comunicazione digitale.

Pertanto, il "nativo digitale" che si introduce da solo nella comunicazione digitale già a partire dai game in rete, si allena a condividere idee, immagini, citazioni, materiale multimediale in ambiente social senza sentire l'esigenza di elaborarli in proprio o senza chiedersi se il proprio modo di interagire in rete sia rispettoso della propria sicurezza, della riservatezza delle informazioni sensibili o del Copyright.

Il CURRICULUM DIGITALE può essere visto come l'insieme di indicazioni utili al raggiungimento della COMPETENZA DIGITALE e di una CITTADINANZA DIGITALE RESPONSABILE per sé e gli altri.

2

La competenza digitale che un alunno dovrebbe raggiungere in età scolare al primo ciclo di istruzione riguarda:

- l'assunzione di responsabilità nell'uso degli strumenti digitali, della comunicazione social e nella cura delle relazioni personali mediate dalla rete;
- il raggiungimento delle abilità all'uso della rete per accedere ad informazioni sicure, certificate, attendibili per accedere alla conoscenza aggiornata in divenire, per risolvere problemi di vita, per vivere meglio e per agire nel rispetto di sé e dell'altro;
- l'acquisizione delle competenze digitali che gli permettono di redigere correttamente un documento strutturato, una presentazione a supporto di una esposizione orale, una raccolta dati e conseguente analisi in formato digitale.

2. RIFERIMENTI NORMATIVI

Per redigere il presente CURRICOLO VERTICALE DIGITALE il Team Digitale e l'Animatrice Digitale si sono basati sui seguenti documenti (NORMATIVA E DOCUMENTI DI RIFERIMENTO):

- a) D.M. n. 254 del 13 novembre 2012 (Indicazioni Nazionali) e Nuovi Scenari 2018;
- b) Raccomandazione 2006/962/CE del Parlamento europeo e del Consiglio (Competenze chiave);
- c) D.M. 107/2015 "La Buona Scuola" che stabilisce il PNSD;
- d) Piano Nazionale Scuola Digitale (PNSD);
- e) DigComp: A Framework for Developing and Understanding Digital Competence in Europe.

"La competenza digitale è ritenuta dall'Unione Europea competenza chiave, per la sua importanza e pervasività nel mondo d'oggi. L'approccio per campi d'esperienza e discipline scelto dalle Indicazioni non consente di declinarla con le stesse modalità con cui si possono declinare le competenze chiave nelle quali trovano riferimento i campi d'esperienza e le discipline formalizzate. Si ritrovano abilità e conoscenze che fanno capo alla competenza digitale in tutti i campi d'esperienza e in tutte le discipline e tutti concorrono a costruirla. Competenza digitale significa padroneggiare certamente le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con "autonomia e responsabilità" nel rispetto degli altri e sapendone prevenire ed evitare i pericoli. In questo senso, tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione." (Raccomandazione del Parlamento Europeo e del Consiglio 18.12.2006).

3. PIANO NAZIONALE SCUOLA DIGITALE (PNSD)

Come riportato nel sito del MIUR, alla pagina della Scuola Digitale, "Il Piano Nazionale 3

Scuola Digitale è un pilastro fondamentale de La Buona Scuola (legge 107/2015), una visione operativa che rispecchia la posizione del Governo rispetto alle più importanti sfide di innovazione del sistema pubblico: al centro di questa visione, vi sono l'innovazione del sistema scolastico e le opportunità dell'educazione digitale".

Questo Piano ha valenza pluriennale e indirizza concretamente l'attività di tutta l'Amministrazione, con azioni già finanziate che saranno prese in carico dalle singole Direzioni del Ministero per l'attuazione; contribuisce a "catalizzare" l'impiego di più fonti di risorse a favore dell'innovazione digitale, a partire dalle risorse dei Fondi Strutturali Europei (PON Istruzione 2014-2020) e dai fondi della legge 107/2015 (La Buona Scuola).

Il PNSD è quindi documento del MI per il lancio di una strategia di innovazione della scuola italiana e del suo sistema educativo nell'era digitale. Di seguito la sintesi.

Il Piano si articola in 4 passaggi: strumenti, competenze e contenuti, formazione, accompagnamento.

- **STRUMENTI:** sono le condizioni che abilitano le opportunità della società dell'informazione e mettono le scuole nelle condizioni di praticarle (accesso, qualità degli spazi e degli ambienti di apprendimento, identità digitale e amministrazione digitale).
- **ACCESSO:** favorire l'accesso e la connessione attraverso la fibra ottica, connettività e cablaggio interno delle scuole.
- **SPAZI E AMBIENTI DI APPRENDIMENTO:** coniugare la crescente disponibilità di tecnologie e competenze abilitanti. Creare ambienti di apprendimento che facilitino apprendimenti attivi e laboratoriali. Sviluppare nuovi modelli e interazione didattica che utilizzi la tecnologia.
- **AMMINISTRAZIONE DIGITALE:** gestione dell'organizzazione scolastica e rafforzamento dei servizi digitali innovativi sul territorio; incremento di funzioni e potenzialità del registro elettronico, esteso a tutto l'Istituto. A tal proposito si evidenzia il collegamento del registro elettronico a Google workspace.
- **IDENTITÀ DIGITALE:** dare un profilo digitale ad ogni persona fisica della scuola. Da settembre 2020 gli account di G-Suite sono stati estesi a tutti gli utenti.

Per ognuno di essi sono stati identificati obiettivi e azioni specifiche. Non si guarda solo all'elemento tecnologico, ma si propone una visione di innovazione che coinvolga in prima persona studenti e personale. Le azioni previste sono organizzate in 9 ambiti di lavoro: accesso, spazi e ambienti per l'apprendimento, identità digitale, amministrazione digitale, competenze digitali degli studenti, imprenditorialità e lavoro, contenuti digitali, formazione del personale, accompagnamento.

Per quanto riguarda la Formazione del personale il PNSD prevede la realizzazione di un percorso di formazione pluriennale centrato sull'innovazione didattica, tenendo conto delle tecnologie digitali come sostegno per la realizzazione di nuovi paradigmi educativi e come mezzo per la progettazione operativa delle attività. L'obiettivo è quello di passare da una scuola della trasmissione a quella dell'apprendimento.

L'ambito n. 2, a cui il Nostro Istituto appartiene, organizza spesso corsi di formazione sul 4

digitale. In tale ottica risulta evidente la necessità di formare prima il personale docente, ricordando l'importanza dell'auto-aggiornamento insito nella funzione docente e nel contratto di lavoro, per poi mirare all'acquisizione delle competenze da parte degli studenti adeguatamente indirizzati dai loro docenti.

L'azione di accompagnamento secondo il PNSD si attua attraverso la nomina di un Animatore Digitale in ogni Istituto, la formazione interna, il coinvolgimento della comunità scolastica, la creazione di soluzioni innovative. Questa figura ha un ruolo strategico anche nella formazione interna del nostro Istituto, con corsi aggiornamento da effettuare durante il triennio di nomina.

4. RUOLO DELL'ANIMATORE DIGITALE E DEL TEAM

DELL'INNOVAZIONE (PNSD)

L'Animatore Digitale è un docente che, insieme al Dirigente Scolastico e al Direttore Amministrativo, avrà il compito di coordinare la diffusione dell'innovazione digitale nell'ambito delle azioni previste dal PTOF triennale e le attività del Piano Nazionale Scuola Digitale.

Individuato dal Dirigente Scolastico di ogni Istituto sarà fruitore di una formazione specifica affinché possa "favorire il processo di digitalizzazione delle scuole nonché diffondere le politiche legate all'innovazione didattica attraverso azioni di accompagnamento e di sostegno sul territorio del piano PNSD". Si tratta quindi di una figura di sistema e non di supporto tecnico (su quest'ultimo infatti il PNSD prevede un'azione finanziata a parte (Azione #26) per la creazione di un Pronto Soccorso Tecnico, le cui modalità attuative devono ancora essere dettagliate).

Il Miur chiede alla figura dell'Animatore Digitale di poter sviluppare progettualità sui seguenti ambiti (cfr. Azione #28 del PNSD):

1. Formazione interna - Stimolare la formazione interna alla scuola sui temi del PNSD, attraverso l'organizzazione e il coordinamento di laboratori formativi favorendo l'animazione e la partecipazione di tutta la comunità scolastica alle attività formative.
2. Coinvolgimento della comunità scolastica - Favorire la partecipazione e stimolare il protagonismo degli studenti nell'organizzazione di attività, anche strutturate, sui temi del PNSD, anche aprendo i momenti formativi alle famiglie e ad altri attori del territorio, per la realizzazione di una cultura digitale condivisa.
3. Creazione di soluzioni innovative - Individuare soluzioni metodologiche e tecnologiche sostenibili da diffondere all'interno degli ambienti della scuola coerenti con l'analisi dei fabbisogni della scuola stessa, anche in sinergia con attività di assistenza tecnica condotta da altre figure (es. uso di particolari strumenti per la didattica di cui la scuola si è dotata, uso di software didattici, uso di applicazioni web per la didattica e la professione, pratica di una metodologia comune basata sulla condivisione via cloud, informazione su percorsi di innovazione e progetti esistenti in

5

altre scuole e agenzie esterne). Coerentemente con quanto previsto dal PNSD (Azione #28), l'animatore digitale dell'Istituto, individuato nella figura della docente Maria Assunta Guida, presenta il piano di intervento suddiviso nel triennio e inserito nel PTOF.

Il nostro Istituto ha provveduto a costituire il TEAM PER L'INNOVAZIONE digitale con i seguenti compiti:

- Supportare e accompagnare l'innovazione didattica nelle istituzioni scolastiche e l'attività dell'Animatore digitale;
- Supportare le attività di formazione interna alla scuola negli ambiti del PNSD, attraverso l'organizzazione di laboratori formativi, favorendo l'animazione e la partecipazione di tutta la comunità scolastica alle attività formative;
- Supportare la partecipazione degli studenti nell'organizzazione di workshop e altre attività, anche strutturate, sui temi del PNSD, anche attraverso momenti formativi aperti alle famiglie e ad altri attori del territorio, per la realizzazione di una cultura digitale condivisa;
- Lavorare in squadra con l'Animatore digitale, individuando soluzioni metodologiche e tecnologiche sostenibili da diffondere all'interno degli ambienti della scuola (es. uso di particolari strumenti per la didattica di cui la scuola si è dotata; la pratica di una metodologia comune; informazione su innovazioni esistenti in altre scuole; un laboratorio di coding per tutti gli studenti) coerenti con l'analisi dei fabbisogni della scuola stessa, anche in sinergia con attività di assistenza tecnica condotta da altre figure.

5. FINALITÀ DELLE TIC: educare ai media

Le finalità formative delle TIC (Tecnologie dell'informazione e della Comunicazione) nella scuola dei tre ordini 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. 6

Nell'ottica di prevenzione del disagio emotivo-relazionale legato all'uso delle tecnologie digitali, fin dalla scuola dell'infanzia è utile promuovere attività didattico-educative finalizzate a sviluppare e potenziare le abilità socio-affettive degli alunni. La scuola ha il compito di far maturare il valore culturale, educativo e formativo legato all'uso delle tecnologie digitali, intese come strumenti che servono a creare una nuova forma di sapere e una nuova organizzazione delle conoscenze. Non si tratta soltanto di insegnare l'uso tecnico di specifici programmi, quanto di far acquisire agli alunni una forma mentis orientata alla comprensione di funzioni generali e alla capacità di saper selezionare e inquadrare le tecnologie digitali nei particolari contesti d'uso. Le TIC dunque, usate in modo appropriato, possono inoltre:

- potenziare l'apprendimento e le prestazioni degli studenti;
- migliorare l'efficacia della mediazione didattica;
- favorire la creazione di situazioni di apprendimento motivanti, coinvolgenti e inclusive;
- sviluppare le diverse intelligenze e i relativi linguaggi promuovendo un apprendimento di tipo individualizzato (e-inclusion);
- aiutare gli studenti a trovare, esplorare, analizzare, interpretare, valutare, condividere, presentare l'informazione in modo responsabile, creativo e con senso critico;
- rendere gli studenti protagonisti nei processi di co-costruzione della conoscenza;
- fornire le competenze necessarie per una cittadinanza attiva e consapevole.

6. COMPETENZE DIGITALI DECLINATE SECONDO LE CINQUE AREE DEL QUADRO DI RIFERIMENTO DigComp (QUADRO COMUNE DI RIFERIMENTO EUROPEO PER LE COMPETENZE DIGITALI) – all'interno della sezione si trovano le competenze in uscita del CURRICOLO DI CITTADINANZA DIGITALE.

La competenza chiave europea analizzata in questo documento è la COMPETENZA DIGITALE che fa riferimento a tutti i campi d'esperienza. Si sottolinea, quindi, come tutti i docenti siano concorrenti al raggiungimento di tale competenza. Quella DIGITALE è una competenza trasversale, fa quindi riferimento a tutte le discipline.

Il DigComp, in particolare, è diventato un riferimento per lo sviluppo e la pianificazione strategica di iniziative sulle competenze digitali, sia a livello europeo sia nei singoli stati membri dell'Unione. Il documento prevede:

- Aree di competenze individuate come facenti parte delle competenze digitali
- Descrittori delle competenze e titoli pertinenti a ciascuna area (21 competenze);
- Livelli di padronanza per ciascuna competenza (i livelli sono 8);
- Conoscenze, abilità e attitudini applicabili a ciascuna competenza;
- Esempi di utilizzo sull'applicabilità della competenza per diversi scopi.

Di seguito le competenze digitali declinate secondo le cinque aree del quadro di riferimento DigComp (Quadro comune di riferimento europeo per le competenze digitali).

1. **INFORMAZIONE:** identificare, localizzare, recuperare, conservare, organizzare e analizzare le informazioni digitali, giudicare la loro importanza e lo scopo.
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 e 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, prendere decisioni informate sui più 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.

La **COMPETENZA DIGITALE** viene anche declinata nelle sue 3 dimensioni (Tecnologica, Cognitiva, Etica) e su questa base vengono inoltre declinati i profili in uscita. La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet.

PROCESSI COGNITIVI FONDANTI LA COMPETENZA

DIMENSIONI

TECNOLOGICA

Uso amichevole e critico delle TSI Conoscenza e comprensione della natura, ruolo e opportunità delle TSI (tecnologie della società dell'informazione)

PAROLE CHIAVE

RICONOSCERE - DISTINGUERE - USARE - INDIVIDUARE - OPERARE - GESTIRE (accedere, prendersi cura del dispositivo, risolvere problemi tecnici) - PREDISPORRE ARCHIVI - UTILIZZARE LA RETE

COGNITIVA

Raccogliere informazioni e saperle usare in modo critico e sistematico.

Consapevolezza della validità e affidabilità delle informazioni

ETICA

Consapevolezza dei principi etici e giuridici impliciti nell'uso interattivo delle TSI nell'impegno all'interazione di comunità e network

RICERCARE - INTERPRETARE - ELABORARE - PROGETTARE - SELEZIONARE - VALUTARE - GIOCARE - VISIONARE - COGLIERE

RISPETTARE - CONDIVIDERE - RACCONTARE - SUPERVISIONARE - VALUTARE I PERICOLI DELLA RETE

7. IL NOSTRO CURRICOLO VERTICALE DIGITALE

Il profilo in uscita dai tre ordini di scuola dell'Istituto Comprensivo è declinato secondo le tre dimensioni della competenza digitale. Attraverso la suddivisione nelle tre dimensioni della competenza digitale viene declinato anche il CURRICOLO DI CITTADINANZA DIGITALE con i rispettivi profili in uscita.

COMPETENZA CHIAVE: Competenza digitale

“La competenza digitale presuppone l'interesse per le tecnologie digitali ed 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” (revisione Consiglio Europeo, maggio 2018).

PROFILO DELLO STUDENTE AL TERMINE DEL PRIMO CICLO DI ISTRUZIONE:

“L'alunno ha buone competenze digitali, usa con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati e informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo.” (Indicazioni Nazionali 2012).

TRAGUARDI FORMATIVI – Indicazioni Nazionali 2012

Al termine della Scuola dell'INFANZIA

Dimostra prime abilità di tipo logico, inizia ad interiorizzare le coordinate spazio temporali e ad orientarsi nel mondo dei simboli, delle rappresentazioni, dei media, delle tecnologie.

Al termine della Scuola PRIMARIA

- Conoscere gli elementi basilari che compongono un computer e le relazioni essenziali fra di essi.
- Utilizzare con dimestichezza e spirito critico le nuove tecnologie
- Usare il computer e la rete per reperire, valutare, produrre, presentare, scambiare informazioni ● Riflettere sulle potenzialità, i limiti e i rischi dell'uso delle tecnologie dell'informazione e della comunicazione

Al termine della Scuola SECONDARIA di I grado

- Utilizzare strumenti informatici e di comunicazione per elaborare dati, testi e immagini e produrre documenti in diverse situazioni;
- Utilizzare la rete per scopi di informazione, comunicazione, ricerca e svago;
- Conoscere le caratteristiche e le potenzialità tecnologiche degli strumenti d'uso più comuni
- Riconoscere vantaggi, potenzialità, limiti e rischi connessi all'uso delle tecnologie più comuni, anche informatiche;
- Utilizzare con spirito critico le nuove tecnologie;

9

COMPETENZE DIGITALI AL TERMINE DELLA SCUOLA DELL'INFANZIA

ABILITA'

TRAGUARDI DI
COMPETENZA

CAMPI DI
ESPERIENZA

- Muovere il mouse e i suoi tasti
- Sapersi orientare tra gli elementi principali del computer e/o tablet e le loro funzioni: tasti delle frecce direzionali, dello spazio, dell'invio
- Prendere visione di lettere e forme di scrittura attraverso il computer e/o tablet
- Utilizzare la tastiera alfabetica e numerica (es.: scrivere il proprio nome)
- Visionare immagini, brevi filmati e documentari didattici
- Sperimentare semplici programmi di grafica
- Ricomporre un'immagine virtuale, per trascinalimento delle varie parti costitutive (puzzle)
- Lettura di una storia e rappresentazione grafica da parte dei bambini su sfondo colorato
- Scoprire ed esplorare le potenzialità offerte dalle nuove tecnologie per giocare, svolgere compiti, acquisire informazioni con la guida e il supporto costante dell'insegnante
- Sperimentar e il coding e introdurre al pensiero computazionale.
- Tutti

VERIFICA E VALUTAZIONE

NOTA: Nella Scuola dell'Infanzia sono previsti momenti di verifica attraverso l'osservazione sistematica.

OBIETTIVI SPECIFICI DI APPRENDIMENTO

CONOSCENZE

- Riconosce e denomina un computer;
- riconosce e denomina le parti principali di un computer: tastiera, mouse, monitor;
- riconosce e denomina una stampante;
- riconosce e denomina una LIM;
- riconosce e denomina un tablet;
- riconosce e denomina un videoproiettore;
- riconosce e denomina dei giochi e degli esercizi interattivi di tipo linguistico, logico, matematico e grafico che svolge al computer, col tablet, alla LIM;
- osserva e discrimina immagini e video presentati dall'insegnante (reali, fantastici, del proprio vissuto, del proprio ambiente...).

METODO

- Il gruppo insegnanti, in base al percorso formativo stabilito e al livello di maturazione dei bambini, stabilirà in itinere le attività e le modalità di approccio alle tecnologie digitali. Esempio: giochi dimovimento e percorsi su grandi scacchiere - pavimento - e griglie (su carta, coding unplugged, o su dispositivo) anche con strumenti strutturati free (Cody Roby, Sapientino doc, Bee-Bot e Blue-Bot, Cubetto).

CURRICOLO SCUOLA PRIMARIA

COMPETENZE DIGITALI PER LA CLASSE PRIMA E SECONDA DELLA SCUOLA PRIMARIA

OBIETTIVI SPECIFICI DI APPRENDIMENTO

COLLEGAMENTI INTERDISCIPLINARI

CONOSCENZE

- conosce le parti principali di un computer e le sue funzioni;
- conosce la funzione di alcuni strumenti tecnologici e il loro impiego in determinate attività didattiche (LIM, videoproiettore, tablet, macchina fotografica digitale...);
- conosce le principali funzioni dei tasti della tastiera (lettere, numeri, spazio, invio, maiuscole-minuscole, segni di punteggiatura, cancellare);
- conosce le funzioni dei tasti del mouse e controlla il puntatore per trascinare e cliccare sugli oggetti interessati;
- conosce le funzioni di base dei programmi di grafica, di giochi didattici, di videoscrittura;
- conosce le icone dei programmi che utilizza e usa correttamente i comandi per aprire e chiudere tali programmi.

ABILITÀ

- Capire le funzioni più elementari del computer e di alcuni strumenti tecnologici ad uso didattico;
- Usare la tastiera e il mouse, anche per sviluppare una buona coordinazione oculo-manuale;
- Utilizzare nelle forme più elementari i programmi di grafica, di giochi didattici, di videoscrittura;
- Dare comandi, avviare e terminare programmi.

TRAGUARDI DI COMPETENZA

- Utilizzare le più comuni tecnologie dell'informazione e della comunicazione per svolgere compiti, acquisire informazioni e potenziare le proprie capacità comunicative.

- Tutte le discipline.

11

METODO

- approccio collaborativo (cooperative learning, problem solving...) per utilizzare tutte le risorse legate alle competenze di alcuni alunni a supporto dei compagni meno esperti e preparati;
- stimolo della creatività e della fantasia, anche attraverso modalità di esecuzione originali e divertenti.

VERIFICA

- Le prove di verifica in itinere sono predisposte per valutare il possesso delle conoscenze e lo stato di sviluppo delle capacità individuali: verifiche pratiche: disegni digitali, uso di strumenti informatici; verifiche scritte: risposte a scelta multipla.

VALUTAZIONE

- La descrizione del livello di competenza è, concordato dagli insegnanti di classe, considerando anche i progressi compiuti rispetto al livello di partenza, l'interesse, l'impegno, la partecipazione e l'attenzione dimostrati nei confronti delle attività.

12

COMPETENZE DIGITALI PER LA CLASSE TERZA, QUARTA E QUINTA DELLA SCUOLA PRIMARIA

CONOSCENZE

- conosce il sistema operativo utilizzato e i più comuni software applicativi;
- conosce le procedure per la produzione di testi, ipertesti, presentazioni, fogli di calcolo;
- conosce le procedure per l'utilizzo di reti informatiche (con supervisione dell'adulto) per ottenere dati e fare ricerche;
- conosce i sistemi di comunicazione mobile (e-mail, chat, social network...) e i rischi ad essi collegati;
- conosce i rischi derivanti da un non corretto utilizzo dei sistemi di comunicazione;
- conosce la procedura per scaricare un documento (download);
- conosce la procedura per salvare un documento in una cartella nominata;
- conosce la procedura per stampare un documento; • conosce la funzionalità di

blocchi logici sempre più complessi (coding).

METODO

OBIETTIVI SPECIFICI DI APPRENDIMENTO	TRAGUARDI DI COMPETENZA	COLLEGAMENTI INTERDISCIPLINARI
ABILITÀ • Utilizzare il sistema operativo installato e i software applicativi, • Utilizzare gli strumenti informatici e di comunicazione per elaborare dati, testi e immagini e produrre documenti; • Utilizzare correttamente le procedure per scaricare, salvare e stampare un documento; • Navigare in Internet per fare ricerche e recuperare dati; • Comunicare attraverso i social mobile conoscendone i rischi e le potenzialità ; • utilizzare il coding per organizzare percorsi o attività sempre più complessi.	• Utilizzare con dimestichezza le più comuni tecnologie dell'informazione e della comunicazione per svolgere compiti, acquisire informazioni e potenziare le proprie capacità comunicative. • Utilizzare il coding in ambito di gioco per sviluppare il pensiero computazionale.	• Tutte le discipline.
VERIFICA	VALUTAZIONE	

- approccio collaborativo (cooperative learning, problem solving...) per utilizzare tutte le risorse legate alle competenze di alcuni alunni a supporto dei compagni meno esperti e preparati;

- stimolo della creatività e della fantasia, anche attraverso modalità di esecuzione originali e divertenti;
- sviluppo del pensiero computazionale;
- lezioni interattive con l'utilizzo della LIM o altri supporti multimediali.
- Le prove di verifica in itinere sono predisposte per valutare il possesso delle conoscenze e lo stato di sviluppo delle capacità individuali:
- verifiche pratiche: disegni digitali,
- uso di strumenti informatici;
- verifiche scritte: esercizi di corrispondenza, risposte a scelta multipla, test, risposte aperte, vero/falso, compilazione di mappe.
- La descrizione del livello di competenza è, concordato dagli insegnanti di classe,

considerando anche i progressi compiuti rispetto al livello di partenza, l'interesse, l'impegno, la partecipazione e l'attenzione dimostrati nei confronti delle attività.

CURRICOLO SCUOLA SECONDARIA DI 1°GRADO

COMPETENZE DIGITALI ALLA FINE DELLA SCUOLA SECONDARIA DI 1°GRADO

OBIETTIVI SPECIFICI DI APPRENDIMENTO

CONOSCENZE

- Utilizza le applicazioni tecnologiche più comuni e le relative modalità di funzionamento;
- utilizza i dispositivi informatici di input e output;
- utilizza sistema operativo, software e app (residenti e/o in cloud), con particolare riferimento ai prodotti anche Open source;
- utilizza con dimestichezza le procedure per la produzione e l'elaborazione di testi, dati, immagini e prodotti multimediali
- produce artefatti digitali (di livelli di complessità commisurati al livello scolastico), utilizzando i programmi e le modalità operative ritenute più adatte al raggiungimento dell'obiettivo;
- utilizza e con dimestichezza le procedure per l'utilizzo della rete Internet per la ricerca di informazioni (motori di ricerca, cloud, e-mail, chat, social network, sistemi di comunicazione mobile, download...);
- è consapevole delle fonti di pericolo nell'utilizzo scorretto dei sistemi di comunicazione di massa, conosce e utilizza le procedure per gestire i propri account in funzione della sicurezza (virus e antivirus) e della privacy (password);
- utilizza con dimestichezza i programmi per il coding e la robotica.

ABILITA' TRAGUARDI DI

COMPETENZA

- Utilizzare con dimestichezza le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall'attività di studio.
- Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie, con particolare riferimento al contesto produttivo, culturale e sociale in cui vengono applicate.
- Saper usare in modo etico gli strumenti per la comunicazione di massa per evitare le possibili minacce alla privacy e altri reati in rete.
- Usare il coding e la robotica per realizzare simulazioni, esercizi, quiz, modellizzazioni... atte allo sviluppo del pensiero computazionale.

METODO	VERIFICA	VALUTAZIONE
• approccio collaborativo (cooperative learning, problem solving...) per utilizzare tutte le risorse legate alle competenze di alcuni alunni a supporto dei compagni meno esperti e preparati; • stimolo della creatività e della fantasia; • sviluppo del pensiero computazionale; • lezioni interattive con l'utilizzo della LIM o altri supporti multimediali; • attività di gruppo, libera o organizzata, con produzione digitale.	• Le prove di verifica in itinere sono predisposte per valutare il possesso delle conoscenze e lo stato di sviluppo delle capacità individuali: • verifiche pratiche: disegni digitali (artistici e tecnici), uso di strumenti informatici, produzione di artefatti; • verifiche scritte: esercizi di corrispondenza, risposte a scelta multipla, test, risposte aperte, vero/falso, elaborazione e compilazione di mappe, documenti da analizzare, schemi da elaborare; • verifiche orali: interrogazioni specifiche su un dato argomento.	• Primo e secondo quadrimestre, in decimi; i voti riportati sul documento di valutazione delle SINGOLE DISCIPLINE, terranno conto, oltre che delle prove svolte in itinere e trasversali, anche dei progressi compiuti rispetto al livello di partenza, l'interesse, l'impegno, la partecipazione e l'attenzione dimostrati nei confronti delle attività digitali. Per le classi in uscita la valutazione confluirà nella competenza digitale acquisita dagli studenti e dalle studentesse.

15

8. VALUTAZIONE DELLA COMPETENZA DIGITALE IN CHIAVE EUROPEE

La competenza digitale, pur associata per gli aspetti più tecnici alla disciplina di tecnologia, consente di essere valutata da tutti i docenti che realizzano attività di carattere digitale ed è uno strumento utile sia per valutare le altre competenze chiave sia le singole discipline.

Il DigComp ha inoltre stabilito i livelli di padronanza per osservare e valutare le competenze digitali dei cittadini riportati nella seguente immagine.

Tabella 1: Principali parole chiave che contraddistinguono i livelli di padronanza

Livelli in DigComp 1.0	Livelli in DigComp 2.1	Complessità dei compiti	Autonomia	Dominio cognitivo
Base Intermedio Avanzato Altamente specializzato	1	Compiti semplici	Con guida	Conoscere
	2	Compiti semplici	Autonomia e guida in caso di necessità	Conoscere
	3	Compiti ben definiti e sistematici, problemi diretti	In autonomia	Comprendere
	4	Compiti e problemi ben definiti e non sistematici	Indipendente e in base alle mie necessità	Comprendere Applicare
	5	Compiti e problemi diversi	Guida per gli altri	
	6	Compiti più opportuni	Capacità di adattarsi agli altri in un contesto complesso	Valutare Creare
	7	Risoluzione di problemi complessi con soluzioni limitate	Integrazione per contribuire alla prassi professionale e per guidare gli altri	

I livelli 7 e 8 non verranno valutati dall'Istituzione scolastica.

Sulla base di questa tabella, sono state elaborate:

1. La rubrica di valutazione della competenza digitale;
2. La griglia di osservazione per rilevare, misurare e valutare la competenza digitale.

Per poter raggiungere i traguardi formativi riportati nelle Indicazioni Nazionali del 2012 e 17

le competenze espresse nel Curricolo Verticale dell'Istituto, si ricorda che che il nostro Istituto utilizza per tutti gli ordini di scuola i seguenti strumenti digitali:

- la PIATTAFORMA DI ISTITUTO "Google Workspace";
- il registro elettronico "Argo".

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.

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare riferimento all'uso delle tecnologie digitali, e indichiamo le misure che la scuola intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori.

Il **"Regolamento Privacy in conformità al Regolamento Generale sulla Protezione dei Dati"** del nostro IC è allineato al "Regolamento UE 2016/679", il cosiddetto "GDPR" (General Data Protection Regulation) e ha recepito il D. Lgs. 30 giugno 2003, n. 196.

Al fine di garantire massima trasparenza e critica presa d'atto rispetto ai temi in questione, al momento dell'iscrizione la Scuola fornisce alle famiglie una "Informativa sul trattamento dei dati personali", ai sensi dell'art. 13 del citato D.Lgs. 196/2003 (Codice della privacy) e dell'art. 13 del Regolamento UE 679/2016 (GDPR).

Come esplicitato nel documento, «il trattamento dei dati personali sarà improntato ai principi di liceità, correttezza, pertinenza, necessità e trasparenza, onde tutelare il diritto alla riservatezza, al decoro e alla reputazione della persona».

I dati personali sono trattati, sia con strumenti elettronici che cartacei, solo ed esclusivamente per le finalità istituzionali della Scuola. Il loro conferimento è obbligatorio per quanto attiene alle informazioni richieste dal modulo base dell'iscrizione, pena l'impossibilità di definire i procedimenti connessi all'iscrizione stessa dell'alunno/a, facoltativo per le informazioni supplementari.

Alle famiglie viene fornita una specifica "Informativa per l'uso delle immagini" con annesso "Modello di autorizzazione" per ogni attività didattica per cui si richieda la necessità di podurre materiale multimediale con immagini delle studentesse e degli studenti, sempre ai sensi del D.Lgs. 196/2003 e del Regolamento UE 679/2016. Il consenso prestato implica il loro utilizzo esclusivamente a fini di documentazione didattica, fermo restando la garanzia che l'immagine in questione sarà

sempre rispettosa della dignità e della personalità del soggetto coinvolto. Sebbene rientranti nel conferimento facoltativo di dati, dunque eccedenti rispetto i trattamenti istituzionali obbligatori, l'eventuale mancato conferimento delle richieste informazioni potrebbe comportare l'impossibilità per la Scuola di erogare efficacemente e in tutte le sue potenzialità il proprio servizio.

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.

PUA (Politica d'Uso Accettabile e Sicura della rete)

Introduzione e processo di revisione

La P.U.A. (Politica d'Uso Accettabile e responsabile di internet) fa parte delle strategie delle Tecnologie di Informazione e Comunicazione (T.I.C.) e si basa su linee guida delle politiche nazionali. Deve essere approvata da Collegio dei Docenti, Consiglio d'Istituto e associazioni di genitori. Il documento inoltre è revisionato su base annuale. I vantaggi di internet a scuola Il curriculum scolastico prevede che gli studenti imparino a trovare materiale, recuperare documenti e scambiare informazioni utilizzando le TIC.

Internet offre sia agli studenti che agli insegnanti una vasta scelta di risorse diverse e opportunità di scambi culturali con gli studenti di altri paesi. Inoltre, su internet si possono recuperare risorse per il tempo libero, le attività scolastiche e sociali. La scuola propone agli studenti e agli insegnanti di utilizzare internet per promuovere l'eccellenza in ambito didattico attraverso la condivisione delle risorse, l'innovazione e la comunicazione. Per gli studenti e per gli insegnanti l'accesso ad internet è un privilegio e un diritto. Poiché esiste la possibilità che gli studenti trovino materiale inadeguato e illegale su internet, la scuola si attiva prendendo delle precauzioni per quanto attiene l'accesso alla rete.

Gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività on-line, di stabilire obiettivi chiari nell'uso di internet insegnando un uso della rete accettabile e responsabile. L'obiettivo principale resta quello di arricchire ed ampliare le attività didattiche, secondo quanto prevede il curriculum scolastico, l'età e la maturità degli studenti. Gli studenti imparano ad utilizzare i metodi di ricerca su internet, che includono i cataloghi per soggetto e l'uso dei motori di ricerca. Ricevere e inviare informazioni o messaggi e-mail prevede una buona abilità di gestione delle informazioni di comunicazione.

Le abilità di gestione delle informazioni includono:

- individuazione di validità, diffusione e origine delle informazioni a cui si accede o che si ricevono;
- utilizzazione di fonti alternative di informazione per proposte comparate;
- ricerca del nome dell'autore, dell'ultimo aggiornamento del materiale, e dei possibili altri link al sito;
- rispetto dei diritti d'autore e dei diritti di proprietà intellettuale.

È quindi necessario che per le classi in cui è previsto l'utilizzo di internet nella didattica curricolare, sia svolto un modulo introduttivo all'utilizzo delle risorse disponibili in rete.

Strategie della scuola per garantire la sicurezza delle TIC

Separazione fisica della rete didattica dalla rete amministrativa. Alla rete amministrativa fanno capo tutti gli uffici e la presidenza mentre a quella didattica afferiscono i laboratori, le sale insegnanti e le aule multimediali. Uso, anche nella didattica, di sistemi operativi che permettono una efficace gestione della multiutenza (Windows, Libre office...).

Il sistema informatico delle TIC della scuola viene regolarmente controllato dallo staff tecnico in base alle norme di sicurezza. La scuola controlla regolarmente i siti visitati ed i file utilizzati su internet.

È vietato inserire file sul server e sui pc o scaricare da internet software non autorizzati o materiale soggetto a diritti di autore (file musicali, video, ecc.);

L'insegnante controlla che venga rispettato questo divieto;

La connessione alla rete esterna prevede un login con password e studenti e docenti devono chiudere la connessione quando hanno terminato il loro lavoro.

Il sistema informatico della scuola è provvisto di un software antivirus aggiornato periodicamente dai responsabili dei laboratori multimediali. Per utilizzare supporti di memorizzazione personali è necessario sottoporli al controllo antivirus.

In generale il software utilizzabile è solamente quello autorizzato dalla scuola, regolarmente licenziato e/o open source (o freeware). Il materiale presente sullo spazio web dedicato alle attività didattiche e su altre piattaforme della scuola è periodicamente controllato dagli amministratori degli stessi.

Il docente, nel preparare una lezione che utilizzi Internet, deve "monitorare" i siti relativi all'argomento per suggerire, poi, quelli più interessanti.

Il docente, durante il collegamento, deve monitorare continuamente il lavoro degli allievi per aiutarli se sono in difficoltà o intervenire in caso di infrazione alle regole. Dall'esempio degli adulti che mostrano un approccio positivo alla rete ed alle sue opportunità, fatto di competenza tecnica, conoscenza e curiosità dei contenuti, consapevolezza dei pericoli ed abilità nello schivarli, gli allievi assorbono tratti importanti della loro identità e imparano a rapportarsi in modo positivo alle nuove tecnologie.

La vigilanza degli spazi "virtuali" scolastici è assimilabile alla vigilanza didattica.

Accertamento dei rischi e valutazione dei contenuti di internet

La scuola si fa carico di tutte le precauzioni necessarie per garantire agli studenti l'accesso a materiale appropriato, anche se non è possibile evitare che gli studenti trovino materiale indesiderato navigando con un computer della scuola.

La scuola non può farsi carico della responsabilità per il materiale trovato su internet o per eventuali conseguenze causate dall'accesso a internet. Gli studenti devono essere pienamente coscienti dei rischi a cui si espongono quando sono in rete. Devono essere educati a riconoscere e a evitare gli aspetti negativi di internet come la pornografia, la violenza, il razzismo e lo sfruttamento dei minori.

Norme e linee guida

Tutti gli utenti che utilizzano internet devono rispettare:

- la legislazione vigente applicata anche alla comunicazione su internet.
- la netiquette (etica e norme di buon uso dei servizi di rete).

Il sistema di accesso a internet della scuola prevede la possibilità di:

- monitorare i siti visitati dagli studenti e dagli insegnanti.

Sono previsti filtri allo stato attuale, presenti nei diversi plessi scolastici. Dal punto di vista tecnico è prevista la presenza di un firewall.

Dopo un certo numero di violazioni delle regole stabilite dalla politica scolastica, la scuola ha il diritto di bloccare l'accesso dell'utente ad internet per un certo periodo di tempo o in modo permanente.

Regole di utilizzo di servizi e-mail

La scuola allo stato attuale fornisce un indirizzo e-mail con dominio icmontemiletto.com, attivato durante il periodo Covid, ai singoli studenti, al personale docente e ATA, ma senza che avvenga la profilazione e richiesta dati sensibili.

L'accesso dai laboratori all'indirizzo di posta elettronica personale è vietato agli studenti salvo circoscritte necessità e previa autorizzazione del docente. Gli studenti non devono rivelare dettagli o informazioni personali loro o di altre persone di loro conoscenza, come indirizzi, numeri di telefono o organizzare incontri fuori dalla scuola. L'invio e la ricezione di allegati è soggetto al permesso dell'insegnante e dal gestore del dominio, il Dirigente Scolastico.

Gestione dei siti web della scuola

Le informazioni pubblicate sui siti della scuola relative alle persone da contattare includono solo l'indirizzo della scuola, l'indirizzo di posta elettronica e il telefono della scuola, ma non informazioni relative agli indirizzi del personale della scuola o altre informazioni del genere. La scuola pubblicherà il materiale prodotto dagli studenti per portare a conoscenza delle famiglie e del territorio l'attività didattica svolta nelle classi solo con il consenso delle famiglie. Si vigilerà con particolare attenzione affinché le fotografie, selezionate per i siti della scuola, non possano essere messe in relazione con l'identità personale degli studenti.

Mailing list moderate, gruppi di discussione e Classroom di Google workspace

La scuola può utilizzare una lista di indirizzi di utenti selezionati per distribuire del materiale. L'insegnante è il moderatore degli altri mezzi di collaborazione, dei gruppi di discussione e delle Classroom di Google workspace qualora siano utilizzati a

scuola. Agli studenti non è consentito l'accesso alle Classroom di Google workspace pubbliche o non moderate. Sono permesse solo Classroom di Google a scopi didattici e comunque sempre con la supervisione dell'insegnante per garantire la sicurezza. Sono disponibili agli studenti solo i gruppi di discussione che hanno obiettivi e contenuti didattici. Altre forme tecnologiche di comunicazione Agli studenti non è permesso utilizzare i telefoni cellulari né altri strumenti tecnologici durante le lezioni o qualsiasi attività didattica.

Servizi on line alle famiglie e utenti esterni

La scuola offre (all'interno di un sito web) tutta una serie di servizi alle famiglie ed agli utenti esterni:

- consultazione elenchi libri di testo;
- orari delle classi, dei docenti, delle strutture;
- comunicazioni alle famiglie;
- reperimento modulistica;
- verifiche online.

Si precisa che tutti i servizi offerti non trattano dati sensibili, ovvero dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Le regole di base relative all'accesso ad internet verranno esposte vicino al laboratorio di informatica. Gli studenti vengono informati dall'insegnante accompagnatore che l'utilizzo di internet è monitorato e verranno date loro delle istruzioni per un uso responsabile e sicuro di internet.

Il personale scolastico viene informato della Politica d'Uso Accettabile della scuola ed è consapevole che l'uso di internet verrà monitorato e controllato. In caso di dubbi legati alla legittimità di una certa istanza utilizzata in internet, l'insegnante dovrà contattare il Dirigente Scolastico o il coordinatore responsabile delle TIC per evitare malintesi. Gli insegnanti saranno provvisti di informazioni concernenti le problematiche sui diritti d'autore che vengono applicate alla scuola.

Informare i genitori/tutori sulla PUA della scuola

I genitori vengono informati sulla PUA della scuola nel sito web della scuola e circolare dirigenziale

Secondo la Legislazione vigente sui Diritti d'Autore Legge del 22 aprile 1941 n° 633 art. 70: "il riassunto, la citazione o la riproduzione di brani o di parti di opera per scopi di critica di discussione ed anche di insegnamento, sono liberi nei limiti giustificati da tali finalità e purché non costituiscano concorrenza all'utilizzazione economica dell'opera". Se nel realizzare delle pagine web all'interno di un'opera originale, l'autore inserisce a scopo di discussione, di critica o di informazione culturale parti di opere, brevi estratti o citazioni (mai l'opera integrale), menzionando chiaramente il nome dell'autore e la fonte, non incorre in problemi di copyright. In questi casi infatti, l'autore delle opere non verrà danneggiato nei suoi diritti ed anzi potrebbe acquistare più notorietà.

Netiquette

Fra gli utenti dei servizi telematici di rete si è sviluppata, nel corso del tempo, una serie di tradizioni e di norme di buon

senso che costituiscono la “Netiquette” che si potrebbe tradurre in “Galateo (Etiquette) della Rete (Net)”: il Galateo della rete.

Ecco alcune regole che TUTTI GLI UTENTI sono invitati a seguire:

1. Non essere offensivo Il testo è l'unico mezzo attraverso il quale comunicare con gli altri in rete. Il tono della voce, l'espressione del viso, non possono essere di aiuto per far comprendere all'altro il senso del discorso. Il rischio di essere fraintesi è altissimo. Bisogna tenerlo sempre presente quando si scrive e usare gli emoticons per ribadire il tono del messaggio: scherzoso, allegro o triste e così via.
2. Seguire le regole di comportamento analoghe alle proprie regole di vita Utilizzare in maniera fraudolenta un prodotto a pagamento equivale ad un furto. Solo acquistandolo regolarmente s'incoraggiano i realizzatori a creare altri prodotti.
3. Scegliere l'ambiente adatto a se stessi - Ogni chat, mailing list, newsgroup, forum ha delle caratteristiche specifiche e non si può trovare sempre argomenti adatti a noi o di nostro interesse. Bisogna, dunque, scegliere la community che si avvicina di più alle proprie esigenze, ma soprattutto quella dove ci si sente più a nostro agio, anche grazie al controllo del moderatore.
4. Scegliere di essere paziente e comprensivo - Quando s'invia un messaggio, non bisogna pretendere risposta. Chi comunica con noi può non essere interessato all'argomento che proponiamo oppure può non avere il tempo di rispondere.
5. Scegliere toni moderati Se si esprime il parere in maniera pacata, è meno probabile che le parole usate possano provocare reazioni dure da chi comunica con noi. Basta poco per infiammare una discussione e serve. Invece, molto tempo per tornare ad un dialogo tranquillo.
6. Rispettare la privacy Usare in rete la stessa regola che usi nella vita. Ognuno di noi ha il diritto di scegliere se condividere o meno le informazioni che lo riguardano, con la consapevolezza che, una volta inviati, messaggi e immagini possono circolare in rete anche in modo virale e distorto.
7. Non abusare delle proprie conoscenze Non usare mai le proprie competenze per entrare nel mondo altrui.
8. Non enfatizzare gli errori degli altri Il desiderio di rispondere velocemente porta a errori di digitazione, di grammatica o di sintassi. Cerchiamo di non commetterli e applichiamo le regole della nostra lingua, ma non enfatizziamo gli errori altrui.
9. Dimenticare le differenze La rete è un mondo nel quale l'unico strumento è la tastiera, l'unico oggetto visibile il monitor. Tutti gli individui sono importanti, a prescindere da ogni differenza.
10. Presentarsi con cura In rete si hanno solo le parole per farsi conoscere. Bisogna usarle con cura, scegliendo quelle di cui si è veramente convinti; solo così daremo a chi comunica con noi la percezione di come siamo veramente.
11. Utilizzare la rete per ampliare le proprie conoscenze Internet è una sterminata enciclopedia a portata di mouse ed offre anche la possibilità di leggere le opinioni degli altri su qualsiasi argomento. Si possono trovare informazioni specialistiche, il materiale per una ricerca scolastica ma anche solo confrontare la propria opinione.
12. Essere prudente Non dare in modo affrettato informazioni personali o che riguardano la propria famiglia. Non accettare senza riflettere di incontrare qualcuno che si è appena conosciuto nella rete. Non credere a tutto quello che viene detto.
13. Non urlare Scrivere in maiuscolo su Internet equivale ad urlare: è uno strumento a disposizione per enfatizzare le cose che stai dicendo. Attenzione a non abusarne.
14. Utilizzare le chat solo per lo scopo per cui sono state create Prima di fare una domanda o di chiedere aiuto agli altri utenti, controllare bene quale sia il posto adatto per farlo e verificare se già non sia stata data in precedenza risposta ad una domanda simile a quella che vorremmo fare noi.

15. Sinteticità e pertinenza Nessuno ha tempo da perdere, soprattutto online, ecco perché ogni intervento deve essere sempre pertinente all'argomento e non eccessivamente lungo.

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.

REGOLAMENTO BYOD

L'azione del Piano Nazionale Scuola Digitale "Politiche attive per il BYOD" (Bring your own device ovvero porta il tuo dispositivo) mira a garantire a tutti gli studenti una formazione digitale che parta dal saper usare i propri dispositivi in maniera consapevole e adeguata.

La scuola digitale, in collaborazione con le famiglie e gli enti locali, deve aprirsi al cosiddetto BYOD (Bring Your Own Device), ossia a politiche per cui l'utilizzo di dispositivi elettronici personali durante le attività didattiche sia possibile ed efficientemente integrato (cfr. azione 6 del PNSD)

Sezione 1 - DECALOGO BYOD (MIUR 2018)

1. Ogni novità comporta cambiamenti. Ogni cambiamento deve servire per migliorare l'apprendimento e il benessere delle studentesse e degli studenti e più in generale dell'intera comunità scolastica.
2. I cambiamenti non vanno rifiutati, ma compresi e utilizzati per il raggiungimento dei propri scopi. Bisogna insegnare a usare bene e integrare nella didattica quotidiana i dispositivi, anche attraverso una loro regolamentazione. Proibire l'uso dei dispositivi a scuola non è la soluzione. A questo proposito ogni scuola adotta una Politica d'Uso Accettabile (PUA) delle tecnologie digitali.
3. La scuola promuove le condizioni strutturali per l'uso delle tecnologie digitali. Fornisce, per quanto possibile, i necessari servizi e l'indispensabile connettività, favorendo un uso responsabile dei dispositivi personali (BYOD). Le tecnologie digitali sono uno dei modi per sostenere il rinnovamento della scuola.
4. La scuola accoglie e promuove lo sviluppo del digitale nella didattica. La presenza delle tecnologie digitali costituisce una sfida e un'opportunità per la didattica e per la cultura scolastica. Dirigenti e insegnanti attivi in questi campi sono il motore dell'innovazione. Occorre coinvolgere l'intera comunità scolastica anche attraverso la formazione e lo sviluppo professionale.
5. I dispositivi devono essere un mezzo, non un fine. È la didattica che guida l'uso competente e responsabile dei dispositivi. Non basta sviluppare le abilità tecniche, ma occorre sostenere lo sviluppo di una capacità critica e creativa.

6. L'uso dei dispositivi promuove l'autonomia delle studentesse e degli studenti.

È in atto una graduale transizione verso situazioni di apprendimento che valorizzano lo spirito d'iniziativa e la responsabilità di studentesse e gli studenti. Bisogna sostenere un approccio consapevole al digitale nonché la capacità d'uso critico delle fonti di informazione, anche in vista di un apprendimento lungo tutto l'arco della vita.

7. Il digitale nella didattica è una scelta: sta ai docenti introdurla e condurla in classe.

L'uso dei dispositivi in aula, siano essi analogici o digitali, è promosso dai docenti, nei modi e nei tempi che ritengono più opportuni.

8. Il digitale trasforma gli ambienti di apprendimento. Le possibilità di apprendere sono ampliate, sia per la frequentazione di ambienti digitali e condivisi, sia per l'accesso alle informazioni, e grazie alla connessione continua con la classe. Occorre regolamentare le modalità e i tempi dell'uso e del non uso, anche per imparare a riconoscere e a mantenere separate le dimensioni del privato e del pubblico.

9. Rafforzare la comunità scolastica e l'alleanza educativa con le famiglie. È necessario che l'alleanza educativa tra scuola e famiglia si estenda alle questioni relative all'uso dei dispositivi personali. Le tecnologie digitali devono essere funzionali a questa collaborazione. Lo scopo condiviso è promuovere la crescita di cittadini autonomi e responsabili.

10. Educare alla cittadinanza digitale è un dovere per la scuola. Formare i futuri cittadini della società della conoscenza significa educare alla partecipazione responsabile, all'uso critico delle tecnologie, alla consapevolezza e alla costruzione delle proprie competenze in un mondo sempre più connesso.

Sezione 2 – Regolamento scolastico per l'attività BYOD.

La tecnologia, se utilizzata in modo responsabile e corretto, fornisce agli studenti opportunità innovative per incrementare la loro cultura, in linea con quanto specificato nel PNSD. L'Istituto vuole favorire tale processo garantendone la sicurezza attraverso una modalità di interazione che contribuisca al miglioramento dell'ambiente educativo e di apprendimento. Pertanto, l'uso improprio dei dispositivi digitali mobili a scuola non è ammesso e viene sanzionato, in relazione alla gravità dell'infrazione, in base a quanto stabilito dal Regolamento di Istituto.

In particolare:

1. Sono ammessi a scuola i seguenti dispositivi: computer portatile, tablet, e-reader. 2. Non sono ammessi a scuola i seguenti dispositivi: videogiochi in genere, cellulari smartphone sono da consegnare all'entrata in classe.

3. I dispositivi (computer, tablet) devono essere usati a scuola per soli scopi didattici e solo con l'autorizzazione dell'insegnante. Agli studenti non è permesso usare dispositivi elettronici per giochi durante le ore scolastiche.

4. Agli alunni non è permesso usare i propri dispositivi al di fuori dell'orario di lezione come ad esempio pause, ricreazione, uscite didattiche, visite guidate, viaggi d'istruzione, attività facoltative extracurricolari, manifestazioni sportive, spettacoli teatrali ecc., se non con l'esplicita autorizzazione del docente responsabile della classe.

5. Gli alunni sono responsabili personalmente dei dispositivi portati a scuola e devono custodirli con cura e attenzione.

6. La scuola non è responsabile della custodia dei dispositivi, di eventuali furti o smarrimenti e di eventuali danni ad essi cagionati dal proprietario o da altri.

7. È in capo agli alunni la responsabilità di riportare a casa il dispositivo al termine delle lezioni. La scuola non assume la responsabilità per la custodia di nessun dispositivo lasciato a scuola.

8. Agli alunni è vietato:

a. usare Internet per scopi diversi da quelli didattici, quando si lavora con i tablet in classe; b. scaricare musica, video e

programmi da Internet o qualsiasi file senza il consenso dell'insegnante;

c. giocare sul computer, in rete o off line (a meno che il gioco non faccia parte di una lezione e sia supervisionato dall'insegnante);

9. Agli alunni è vietato inoltre:

utilizzare la Rete e i social network per deridere, offendere, denigrare compagni, docenti, personale scolastico, parenti/amici dei compagni; si ricorda che il cyberbullismo è un reato e qualsiasi atto degli studenti che dovesse configurarsi come reato verrà denunciato d'ufficio alle autorità competenti, ad esempio forze dell'ordine.

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/le 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.

L'Istituto Comprensivo "Montemiletto", in ottemperanza alla normativa vigente e soprattutto alle specifiche leggi in materia di prevenzione e contrasto al bullismo e cyberbullismo, la n.71/2017 e n.70/2024, è caratterizzato dalla presenza di un team per le emergenze che ha la responsabilità della presa in carico dei fenomeni. Il team, quindi, raccoglie la segnalazione che può giungere dalla vittima, dal sostenitore della vittima, dal genitore, dall'insegnante e/o da altre figure presenti nella scuola; nella segnalazione si valuta la presenza o meno del gruppo anche attraverso una descrizione concreta degli episodi di prepotenza. In seguito il team valuta la gravità del fenomeno per decidere l'intervento da attuare: mette in atto la prevenzione selettiva, rivolta ai sottogruppi a rischio oppure la prevenzione indicata, indirizzata a studenti e studentesse con problematiche specifiche. In tale fase di gestione del caso, la scuola richiede la collaborazione dei servizi del territorio attraverso figure professionali, quali psicologo, educatore. Inoltre per tutelare il benessere psicofisico del minore, si richiederà la rimozione/l'oscuramento dei contenuti lesivi mediante il gestore della rete e/o il Garante per la protezione dei dati personali.

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 minorenni.

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.

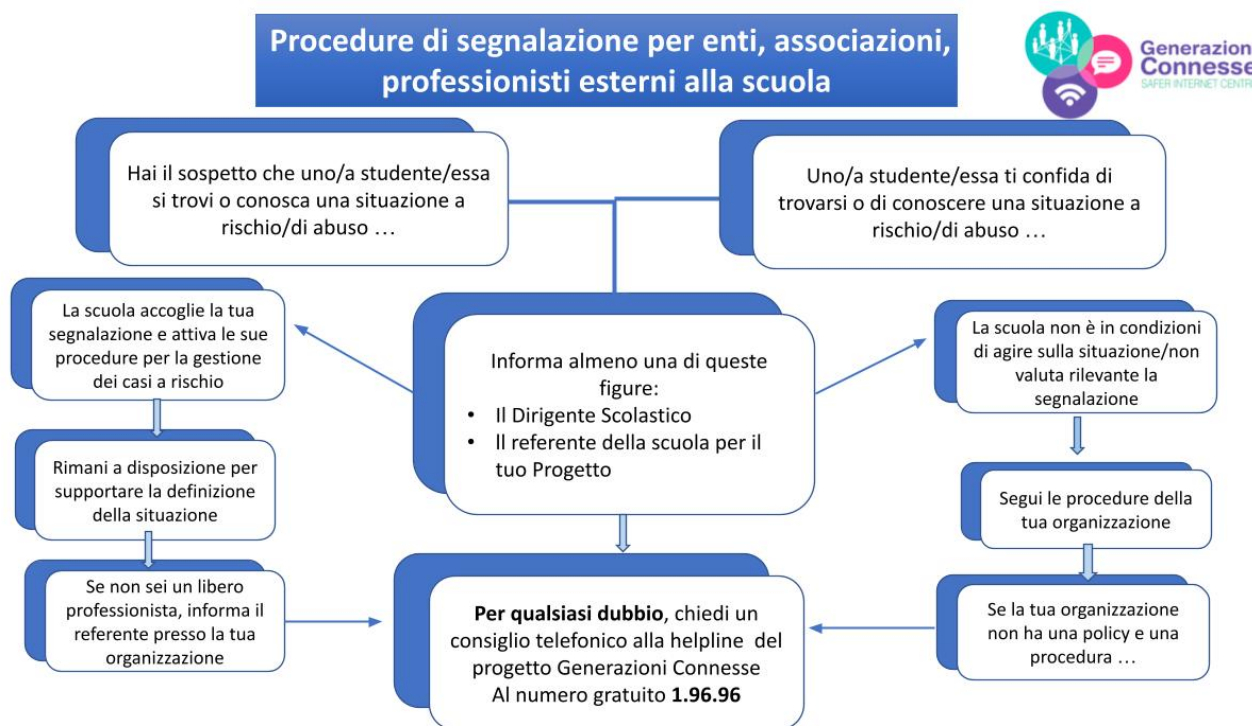
Strumenti a disposizione di studenti/esse

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 condivide 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.

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.

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).

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

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

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.

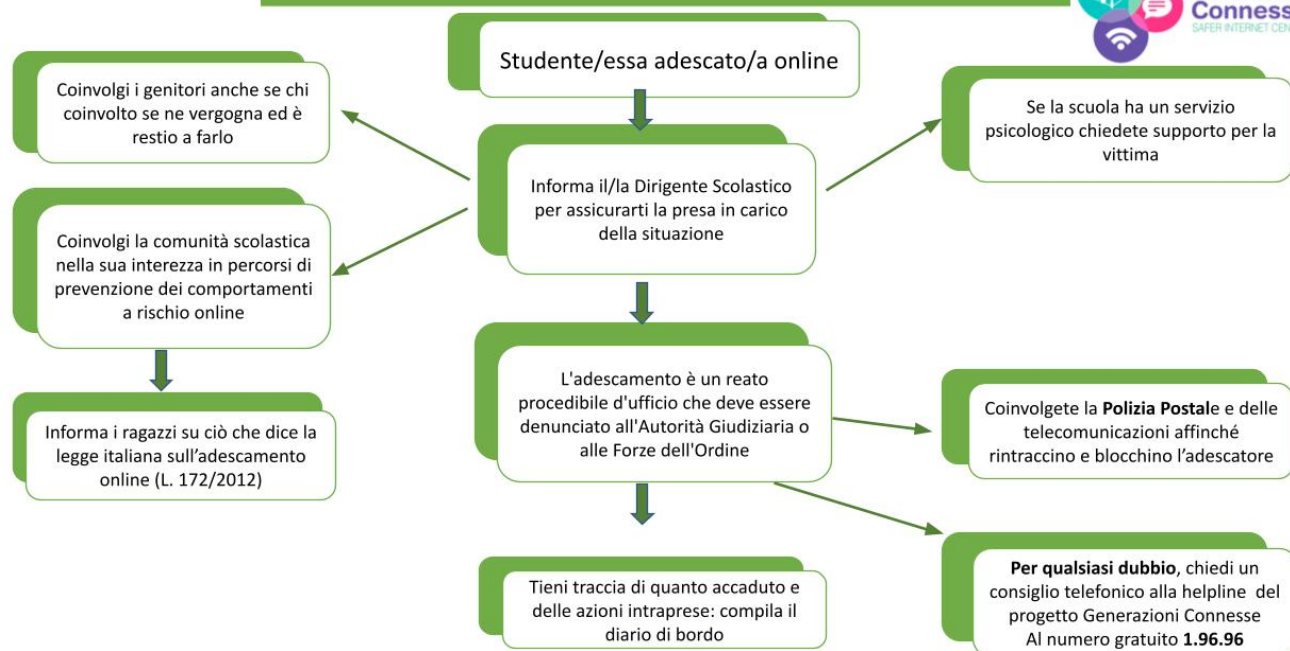
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

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

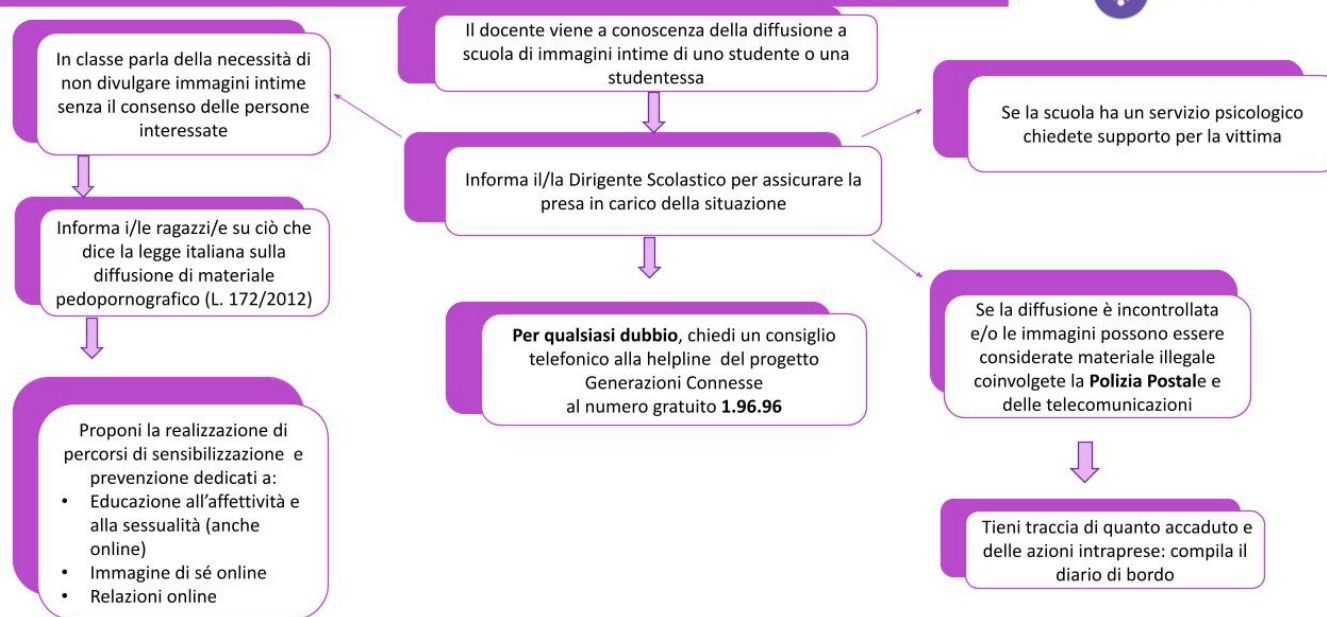
Se emergono evidenze passa allo schema successivo

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

Procedure interne: cosa fare in caso di Adescamento Online?



Procedure interne: cosa fare in caso di diffusione non consensuale di immagini intime?



L'Istituto Comprensivo "Montemiletto" attraverso il team delle emergenze, raccolta la segnalazione e determinata la forma di cyberbullismo agito ai danni del minore, qualora il fatto accaduto costituisca reato, segnala l'evento all'autorità giudiziaria e/o alla Polizia Postale per vagliare i contenuti, ricevuti e/o trasmessi, e la sistematicità di diffusione in rete. Inoltre, richiede l'intervento di figure professionali sul territorio e/o autorità competenti soprattutto se il cyberbullismo va oltre il contesto

scolastico. Altri strumenti indispensabili che la scuola individua per la gestione dei casi di cyberbullismo, derivano dalla piattaforma Elisa e da Generazioni Connesse.