Documento di ePolicy

PAIC8AS004

I.C.S. MARGHERITA HACK -PA

VIA CESARE TERRANOVA N. 93 - 90131 - PALERMO - PALERMO (PA)

TIZIANA DINO

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

1. **Presentazione dell'ePolicy**
    1. Scopo dell'ePolicy
    2. Ruoli e responsabilità
    3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
    4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

5. Gestione delle infrazioni alla ePolicy
6. Integrazione dell'ePolicy con regolamenti esistenti
7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

2. **Formazione e curricolo**
    1. Curricolo sulle competenze digitali per gli studenti
    2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
    3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
    4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
    1. Protezione dei dati personali
    2. Accesso ad Internet
    3. Strumenti di comunicazione online
    4. Strumentazione personale
4. **Rischi on line: conoscere, prevenire e rilevare**
    1. Sensibilizzazione e prevenzione
    2. Cyberbullismo: che cos'è e come prevenirlo
    3. Hate speech: che cos'è e come prevenirlo
    4. Dipendenza da Internet e gioco online
    5. Sexting
    6. Adescamento online
    7. Pedopornografia
5. **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

Perché è importante dotarsi di una E-policy?

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

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

L'Istituto Comprensivo Statale "Margherita Hack" ha elaborato questo documento in conformità con le "Linee di orientamento per la prevenzione e il contrasto dei fenomeni di Bullismo e Cyberbullismo", decreto prot. N. 18 del 13 gennaio 2021,

con l'obiettivo di educare e sensibilizzare gli alunni, gli insegnanti e i genitori all'uso sicuro e consapevole di Internet. Infatti lo sviluppo delle Nuove Tecnologie, il loro utilizzo nell'ambito didattico e la maggiore diffusione nella vita di tutti i giorni di questi strumenti richiede maggiore responsabilità e consapevolezza. È compito dell'intera comunità scolastica, genitori inclusi, garantire che gli studenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato e sicuro. Di qui la necessità di dotare la Scuola di una propria Policy di E-safety, per gestire le eventuali infrazioni come integrazione del Regolamento d'Istituto.

1.2 - Ruoli e responsabilità

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

Nel documento di ePolicy sono definiti con chiarezza ruoli, compiti e responsabilità di ciascuna delle figure professionali all'interno dell'Istituto che, a vario titolo, si occupano di gestione e programmazione delle attività formative, didattiche ed educative e di tutte quelle figure appartenenti alla comunità educante.

IL DIRIGENTE SCOLASTICO

Nel promuovere l'uso consentito delle tecnologie e di internet, il ruolo del Dirigente Scolastico è quello di:

- promuovere la cultura della sicurezza online fornendo il proprio contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo e del cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC;
- coinvolgere, nella prevenzione e contrasto al fenomeno, tutte le componenti della comunità scolastica, particolarmente quelle che operano nell'area dell'informatica, partendo dall'utilizzo sicuro di Internet a scuola;
- prevedere all'interno del PTOF corsi di aggiornamento e formazione in materia di prevenzione dei fenomeni del bullismo e cyberbullismo e uso consapevole delle TIC rivolti al personale docente e non docente;
- prevedere azioni culturali ed educative rivolte agli studenti, per acquisire le competenze necessarie all'esercizio di una cittadinanza digitale consapevole.

Il Dirigente Scolastico, inoltre, ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di uso improprio delle tecnologie digitali e di informare tempestivamente i soggetti esercenti la responsabilità genitoriale ovvero i tutori dei minori coinvolti, attivando adeguate azioni di carattere educativo (art. 5, comma 1, legge 71/2017).

L'ANIMATORE DIGITALE

L'Animatore digitale:

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

IL REFERENTE PER LA PREVENZIONE ED IL CONTRASTO AL BULLISMO E CYBERBULLISMO

Il ruolo del referente per Bullismo e Cyberbullismo include i seguenti compiti:

- coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo;
- promuove la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale;
- coordina le attività di prevenzione ed informazione sulle sanzioni previste e sulle responsabilità di natura civile e penale, anche con eventuale affiancamento di genitori e studenti;
- si rivolge a partner esterni alla scuola, quali servizi sociali e sanitari, aziende del privato sociale, forze di polizia, per realizzare un progetto di prevenzione;
- cura rapporti di rete fra scuole per eventuali convegni, seminari, corsi.

Il Referente bullismo e cyberbullismo può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio.

I DOCENTI

I Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete, integrando parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica.

Loro è il compito di accompagnare e supportare gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete 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.

IL PERSONALE AMMINISTRATIVO, TECNICO E AUSILIARIO (ATA)

Il personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il Dirigente scolastico e con il personale docente tutto. Diverse figure che, in sinergia, si occupano ciascuno per la propria funzione, del funzionamento dell'Istituto

scolastico che passa anche attraverso lo sviluppo della cultura digitale e dell'organizzazione del tempo scuola. Esiste un concreto coinvolgimento del personale nelle attività di formazione e autoformazione in tema di bullismo e cyberbullismo. Il personale ATA, infatti, insieme ad altre figure, è coinvolto nella segnalazione di comportamenti non adeguati e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo e cyberbullismo.

GLI STUDENTI E LE STUDENTESSE

Gli studenti e le studentesse, in relazione al proprio grado di maturità e consapevolezza raggiunta:

- utilizzano al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti;
- imparano le regole basilari, per rispettare gli altri, quando sono connessi alla rete, facendo attenzione alle comunicazioni che inviano;
- imparano a tutelare e rispettare online se stessi ed i propri compagni;
- sono coinvolti nella progettazione e nella realizzazione delle iniziative scolastiche che riguardano l'uso positivo delle TIC e della Rete, al fine di favorire un miglioramento del clima e, dopo opportuna formazione, possono operare come tutor per altri studenti;
- si impegnano a diffondere buone pratiche nel rispetto dei diritti di ogni membro della comunità scolastica ed extrascolastica.

I GENITORI

I genitori, in continuità con l'Istituto scolastico:

- partecipano attivamente alle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali;
- vigilano sull'uso delle tecnologie da parte dei ragazzi, con particolare attenzione ai tempi, alle modalità, agli atteggiamenti conseguenti;
- si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicano con loro circa i problemi rilevati quando i propri figli non usano responsabilmente le tecnologie digitali o Internet;
- conoscono le azioni messe in campo dalla scuola e collaborano secondo le modalità previste dai diversi Regolamenti e dal presente Documento di ePolicy.

GLI ENTI EDUCATIVI ESTERNI E LE ASSOCIAZIONI

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola:

- si conformano alla nostra politica riguardo all'uso consapevole della Rete e delle TIC;
- promuovono comportamenti sicuri, la sicurezza online e assicurano la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

Per quanto non espressamente indicato sui ruoli e sulle responsabilità delle figure presenti all'interno dell'Istituzione scolastica, si rimanda:

- all'art. 21, comma 8, Legge 15 marzo 1997, n. 59;
- all'art. 25 della Legge 30 marzo 2001, n. 165; al CCNL in vigore;
- al D.P.R. 8 marzo 1999, n. 275;

- alla Legge 13 luglio 2015, n. 107;
- al Piano Nazionale Scuola Digitale;
- a quanto statuito in materia di culpa in vigilando, culpa in organizzando, culpa in educando.

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

Tutti gli attori che entrano in relazione educativa con gli 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).

Gli Enti educativi esterni e le associazioni che entrano in relazione con il nostro Istituto devono conformarsi alla nostra politica riguardo all'uso consapevole della Rete e delle TIC e, inoltre, devono promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

Le attività progettuali o di formazione a carattere seminariale, devono essere preventivamente autorizzate dal Dirigente scolastico, con modalità e tempi concordati con il Referente d'Istituto per il contrasto del Bullismo e Cyberbullismo; a tal proposito, al fine di verificare preventivamente il contenuto da somministrare o dibattere con la scolaresca, i soggetti esterni forniranno un dettagliato programma delle attività con narrazione sintetica della scaletta, al fine di ottenerne l'autorizzazione dalla Dirigenza.

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

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

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

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

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

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

Il documento di E-Policy è stato redatto dal gruppo di lavoro composto dai docenti Piero Romano (Animatore Digitale), Valeria Anzelmo, Silvia Melodia, Luciano Campo e coordinato dal Referente per la prevenzione ed il contrasto del bullismo e cyberbullismo, ins.te Sabatino Carmela. I docenti componenti il gruppo di lavoro hanno seguito una formazione online apposita, che ha valore di guida informativa sulla realizzazione dello stesso percorso.

Il presente documento, frutto di collaborazione e confronto, sarà oggetto di condivisione da parte dell'intera comunità scolastica attraverso l'approvazione degli Organi Collegiali; le norme adottate e sottoscritte dalla scuola in materia di sicurezza ed utilizzo delle tecnologie digitali, saranno rese note tramite pubblicazione del presente documento sul sito web della scuola, dandone così ampia diffusione a tutta la Comunità Scolastica.

1.5 - Gestione delle infrazioni alla ePolicy

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

Sono oggetto di condotte sanzionabili, in relazione all'uso improprio delle TIC, dei dispositivi e della Rete a scuola da parte degli studenti e delle studentesse, fermo restando il Regolamento d'Istituto:

- la condivisione online di immagini o video di compagni, compagne e personale della scuola senza il loro esplicito consenso o che li ritraggono in pose offensive e denigratorie;
- la condivisione di scatti intimi ed a sfondo sessuale;
- la condivisione di dati personali;
- l'invio di immagini o video, volti all'esclusione di compagni e compagne.

Tutte le infrazioni andranno tempestivamente segnalate al Dirigente Scolastico, anche tramite il Referente al contrasto del bullismo e cyberbullismo, che avrà cura di convocare le parti interessate onde valutare le possibili azioni da intraprendere.

Si farà riferimento a quanto previsto dal Regolamento d'Istituto, procedendo all'applicazione delle eventuali sanzioni in maniera graduata, proporzionalmente alla gravità dei fatti:

- Richiamo verbale
- Sanzioni estemporanee commisurate alla gravità della violazione commessa (assegnazione di attività aggiuntive da svolgere a casa sui temi di Cittadinanza e Costituzione o Educazione Civica)
- Nota informativa ai genitori o tutori mediante registro elettronico
- Convocazione dei genitori o tutori per un colloquio con l'insegnante
- Convocazione dei genitori o tutori per un colloquio con il Dirigente Scolastico

Episodi di cyberbullismo o di altri reati online saranno trattati in conformità con quanto previsto dalla legge.

Le sanzioni avranno come carattere preferenziale sempre quello educativo/riabilitativo e dovranno essere considerate quali occasioni di recupero.

La Scuola prenderà e manterrà nel tempo tutte le precauzioni necessarie e adatte per garantire agli studenti l'accesso a materiale e ambienti appropriati, anche se è impossibile evitare in assoluto che essi trovino materiale indesiderato navigando su 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 ad internet.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

Si rimanda al Regolamento d'Istituto ed al Regolamento Bullismo e Cyberbullismo L.71/2017 e L.70/2024.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il monitoraggio dell'implementazione della Policy e del suo eventuale aggiornamento sarà curato dal Dirigente Scolastico con la collaborazione dell'Animatore digitale, del Team e del Referente del bullismo e cyberbullismo.

Avrà il fine di rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di Internet. Il monitoraggio on-line sarà rivolto anche ai docenti, al fine di valutare l'impatto della Policy e la necessità di eventuali miglioramenti. L'aggiornamento della Policy sarà curato dal Dirigente scolastico, dall'Animatore digitale, dal Team, dal Referente al contrasto del bullismo e cyberbullismo e dagli Organi Collegiali.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- organizzare incontri periodici del gruppo di lavoro ePolicy
- realizzazione di un sistema di monitoraggio delle attività
- organizzare un evento di presentazione del progetto Generazioni Connesse rivolto agli studenti.

Azioni da svolgere nei prossimi 3 anni:

- organizzare eventi di presentazione del progetto Generazioni Connesse rivolto agli studenti, ai genitori ed ai docenti.

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

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

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

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

Le competenze digitali richiamano diverse dimensioni sulle quali sarà possibile lavorare in classe, in un'ottica che integra la dimensione tecnologica con quella cognitiva ed etica. Nello specifico:

- dimensione tecnologica: è importante far riflettere i più giovani sul potenziale delle tecnologie digitali come strumenti per la risoluzione dei problemi della vita quotidiana, onde evitare automatismi che abbiano conseguenze incerte, attraverso un'adeguata comprensione della "grammatica" dello strumento.
- dimensione cognitiva: fa riferimento alla capacità di creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità.
- dimensione etica sociale: la prima fa riferimento alla capacità di gestire in modo sicuro i propri dati personali e quelli altrui, e di usare le tecnologie digitali per scopi eticamente accettabili e nel rispetto degli altri. La seconda, invece, pone un po' più l'accento sulle pratiche sociali e quindi sullo sviluppo di particolari abilità sociocomunicative e partecipative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di coloro con cui comunichiamo online.

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 ciber-sicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico.

2.2 - Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

Risulta molto importante, infatti, che vi sia una particolare attenzione all'uso delle TIC nella didattica; un loro utilizzo strutturato e integrato può rendere gli apprendimenti motivanti, coinvolgenti ed inclusivi e, al contempo, permette al docente di guidare studenti e studentesse nella fruizione dei contenuti online, che è ormai la modalità naturale di apprendimento al di fuori della scuola. Le TIC, inoltre, permettono di sviluppare capacità che sono più importanti anche in ambito lavorativo, come il lavoro di gruppo anche a distanza e il confronto fra pari in modalità asincrona.

Il corpo docente ha partecipato a corsi di formazione anche nell'ambito di Piani Nazionali e ad iniziative organizzate dall'Istituzione e possiede generalmente una buona competenza di base e, nel caso di alcune figure (Animatore digitale e Team), anche di carattere specialistico. È inoltre disponibile ad aggiornarsi, in quanto il percorso complesso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica non si può esaurire in breve tempo, dato il progresso galoppante delle tecnologie. Perciò sono previsti momenti di autoaggiornamento, momenti di formazione personale o collettiva anche all'interno dell'Istituto, con la condivisione delle conoscenze dei singoli e il supporto dell'Animatore digitale e del Team previsto dal PNSD e corsi di aggiornamento online.

2.3 - Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

Il nostro Istituto si avvale della figura dell'Animatore digitale che, con il Dirigente Scolastico e il D.S.G.A., collabora per raggiungere gli obiettivi di innovazione del PNSD nella scuola. Inoltre, a partire dall'anno scolastico 2017-2018 è attiva la figura del Referente d'Istituto per le attività di prevenzione e contrasto al bullismo e al cyberbullismo (L.107/2015).

Si rende, comunque, necessaria la formazione di tutti i docenti sull'uso consapevole e sicuro di Internet e sui rischi della rete. Infatti il percorso di formazione specifica dei docenti non può essere esaustivo, ma deve essere permanente in relazione all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono in maniera costante ed autonoma i ragazzi. Può prevedere momenti di autoaggiornamento e di formazione personale o collettiva, ma in futuro la scuola supporterà la formazione attraverso corsi interni o esterni, mediante seminari, conferenze e dibattiti. Non si escluderà la formazione a distanza né la partecipazione ad iniziative al di fuori della programmazione d'Istituto

L'uso consapevole e sicuro della Rete e delle tecnologie digitali e la costruzione di percorsi formativi pensati ad hoc per i docenti, si concretizzano in alcune azioni da portare avanti nel triennio.

Nell'ottica di una vera e propria programmazione, con azioni specifiche, ci si propone, per esempio, di:

- analizzare il fabbisogno formativo degli insegnanti sull'uso sicuro della rete;
- promuovere la partecipazione dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto "Generazioni Connesse";
- organizzare incontri con professionisti della scuola o con esperti esterni, enti/associazioni, ecc.

2.4. - Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

A tale proposito è importante informare i genitori sulle condotte che si dovranno adottare a scuola e, in generale, offrire loro consigli da mettere in pratica con i propri figli. Attraverso consigli, indicazioni e informazioni su iniziative e azioni della scuola, in riferimento ai rischi connessi ad un uso distorto della Rete da parte degli studenti, prevediamo di:

- **elaborare regole sull'uso delle tecnologie digitali** da parte dei genitori nelle comunicazioni con la scuola e con i docenti (es. email, gruppo whatsapp, sito della scuola ecc.) e informarli adeguatamente anche riguardo alle regole per gli studenti e le studentesse;
- **fornire ai genitori consigli o linee guida sull'uso delle tecnologie digitali nella comunicazione** con i figli e in generale in famiglia, facendo anche riferimento alla sezione dedicata ai genitori del sito www.generazioniconnesse.it
- **organizzare percorsi di sensibilizzazione e formazione dei genitori** su un uso responsabile e costruttivo della Rete in famiglia e a scuola.

Scuola e famiglia sono chiamate a collaborare per garantire la crescita formativa di ciascun alunno, perciò stipulano all'inizio dell'anno scolastico il Patto Educativo di Corresponsabilità. Alla luce del progresso e dell'evoluzione delle tecnologie, l'Istituto attiverà iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine saranno previsti incontri fra docenti e/o esperti e genitori sui temi oggetto della Policy per la diffusione del materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati (Generazioni Connesse) e dalle forze dell'ordine. Sul sito della scuola, inoltre, sarà pubblicato il presente documento per la divulgazione delle informazioni e delle procedure contenute, per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'Istituto e per prevenire i rischi legati ad un utilizzo scorretto di Internet.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2024/2025)

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

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

- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

personali.

All'atto dell'iscrizione nel nostro Istituto, ai genitori vengono fornite l'informativa e la richiesta di autorizzazione all'utilizzo dei dati personali degli alunni (eccedenti i trattamenti istituzionali obbligatori), come ad esempio l'utilizzo di fotografie, video o altri materiali audiovisivi contenenti l'immagine e/o il nome del proprio figlio all'interno di attività educative e didattiche per scopi documentativi, formativi e informativi, durante gli anni di frequenza della scuola.

Nell'informativa si specifica che le immagini e le riprese audiovideo realizzate dalla scuola, nonché gli elaborati prodotti dagli studenti durante le attività scolastiche, potranno essere utilizzati esclusivamente per documentare e divulgare le attività della scuola tramite il sito Internet di Istituto. L'autorizzazione non consente l'uso dell'immagine in contesti che pregiudichino la propria dignità personale ed il decoro e comunque per uso e/o fini diversi da quelli sopra indicati. Inoltre, in caso di partecipazioni a concorsi o manifestazioni l'Istituto richiede apposita autorizzazione, chiaramente distinguibile da altre richieste o dichiarazioni. La formula utilizzata per chiedere il consenso è, in ogni caso, comprensibile, semplice e chiara.

Pertanto, in ottemperanza al GDPR (General Data Protection Regulation) e al D. Lgs. 10 agosto 2018, n. 101, entrato in vigore il 19 settembre, la scuola non si impegna solo a tutelare la privacy degli studenti e delle loro famiglie, ma anche ad informare e soprattutto rendere consapevoli gli studenti di quanto sia importante tutelare il diritto alla riservatezza di sé stessi e degli altri.

Dall'informativa sul trattamento dei dati personali e dalle linee guida per il trattamento e la protezione dei dati personali si evincono le finalità del trattamento stesso:

- gestione delle attività propedeutiche all'avvio dell'anno scolastico;
- gestione delle attività didattica-formativa e di valutazione;
- gestione di attività socio-assistenziali (con particolare riferimento a soggetti che versano in condizioni di disagio sociale, economico o familiare);
- gestione di mense scolastiche o fornitura di sussidi, contributi e materiale didattico;
- partecipazione di tutte le attività organizzate in attuazione del Piano dell'Offerta Formativa;
- gestione del contenzioso tra la scuola e la famiglia dell'alunno;
- inviare comunicazioni via email o via sms relative a informazioni riguardanti lo studente, dietro prestazione del suo libero consenso;
- comunicare i dati personali dello studente ad altri enti per agevolare l'orientamento, la formazione e l'inserimento professionale, dietro prestazione del suo libero consenso.

Dagli stessi documenti si desume che l'incaricato del trattamento dati dovrà:

- accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni;
- trattare i dati personali in modo lecito e secondo correttezza;
- raccogliere e registrare i dati personali per scopi determinati, espliciti e legittimi, ed utilizzarli solo per operazioni di trattamento compatibili con le finalità connesse all'attività svolta;
- verificare che i dati siano esatti, aggiornandoli nel caso in cui si renda necessario, e che siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e

successivamente trattati;

- conservare i dati in forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;
- comunicare o eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati e riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute;
- fornire sempre l'informativa agli interessati, ai sensi degli artt.13 e 14 del Regolamento UE 2016/679, utilizzando i moduli appositamente predisposti;
- accertarsi che gli interessati abbiano autorizzato l'uso dei dati richiesti;
- informare prontamente il referente privacy di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati;
- accertarsi dell'identità degli interessati e della loro autorizzazione al trattamento al momento del ritiro di documentazione in uscita;
- non fornire telefonicamente o a mezzo fax dati e informazioni senza avere la certezza dell'identità del destinatario;
- non lasciare a disposizione di estranei documenti o supporti di memorizzazione che contengono dati personali o sensibili;
- accertarsi della distruzione di documenti inutilizzati contenenti dati personali o sensibili;
- non abbandonare la postazione di lavoro, senza aver provveduto a custodire in luogo sicuro i documenti contenenti dati personali (es. archivi o contenitori muniti di serratura).

3.2 - Accesso ad Internet

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

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

2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

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

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

L'accesso a Internet è possibile e consentito per la didattica in tutti i plessi della primaria e della secondaria di primo grado attraverso reti WiFi.

Il Regolamento d'Istituto della nostra scuola prevede una parte dedicata all'uso di Internet in cui gli studenti si impegnano a:

- accedere a Internet solo in presenza e con il controllo di un docente;
- non scaricare file musicali, foto, filmati e file multimediali, salvo quelli necessari per finalità didattiche, e comunque, prima di scaricare documenti o file da Internet a chiedere autorizzazione al docente;
- utilizzare le postazioni dell'Istituto per accedere in Internet solo per scopi didattici;
- non alterare le opzioni del software di navigazione;
- a chiedere sempre il permesso al docente prima di iscriversi a qualche concorso o prima di riferire l'indirizzo della scuola.

Sempre dal Regolamento d'Istituto, si evince che le postazioni prevedono una configurazione del software di navigazione con limitazione ai siti proibiti e che l''accesso a Internet, anche da parte degli adulti, può avvenire solo per motivi connessi all'attività didattica e alla formazione.

3.3 - Strumenti di comunicazione online

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

Grazie agli strumenti di comunicazione online è possibile usufruire dell'interattività del mezzo, superare le barriere spazio-temporali, usare un linguaggio multimediale, ipertestuale e accattivante, promuovere la partecipazione e il coinvolgimento dei diversi attori in gioco nel processo educativo. I diversi strumenti di comunicazione online rispondono alle necessità di comunicazione interna e di comunicazione esterna.

Molti strumenti di comunicazione online possono essere utilizzati dalla scuola, sia per raggiungere soggetti esterni, al fine di valorizzare e promuovere le attività portate avanti dall'Istituto (istituzioni, famiglie, studenti non ancora iscritti, associazioni, ecc.) sia per far circolare all'interno della scuola informazioni di servizio o contenuti importanti fra i diversi attori scolastici (docenti, studenti, genitori, collaboratori scolastici, ecc.).

Fra gli strumenti di **comunicazione esterna** troviamo in primis il sito web della scuola, utilizzato soprattutto per fornire informazioni di servizio rivolte a studenti o genitori. La scuola, in qualità di ente pubblico, divulga sul proprio sito web i contenuti che sono di volta in volta valutati come pertinenti alle finalità educative istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative.

Il sito del nostro Istituto Comprensivo è raggiungibile all'indirizzo https://icmargheritahackpa.edu.it La gestione del sito e la rispondenza alle normative per quanto concerne i contenuti (accuratezza, appropriatezza, aggiornamento) e le tecniche di realizzazione e progettazione è a cura del docente referente della pagina web. Sul sito è possibile trovare documenti quali: il Regolamento d'Istituto, il PTOF (Piano triennale per l'Offerta formativa), il PAI (Piano Annuale per l'Inclusione), il PNSD (Piano nazionale Scuola Digitale), il Regolamento Bullismo e Cyberbullismo, il RAV e il Curricolo d'Istituto. Sull'homepage del sito, inoltre sono sempre in evidenza eventi, avvisi ai genitori, documentazione di attività curricolari ed extracurricolari svolte; pulsanti attivi permettono l'accesso a link di interesse, tra cui il Registro Elettronico, le attività della scuola e le piattaforme eTwinning, Safe Internet Day ed Erasmus+. Sempre dall'homepage è possibile accedere all'area riservata del sito dove sono caricate le comunicazioni interne. L'accesso a tale area è nominativo, con credenziali diverse per ogni utente.

Anche il Registro elettronico è uno strumento di comunicazione con le famiglie e gli studenti che vi possono accedere attraverso credenziali individuali fornite dalla scuola da modificare al primo accesso. Altrettanto efficace nell'ambito della comunicazione esterna è la piattaforma G-suite destinata alla didattica, alla messaggistica ed agli incontri con i genitori.

Tra i diversi strumenti di **comunicazione interna**, il nostro Istituto ha adottato:

- **il Registro elettronico** con tutte le funzionalità che la sua piattaforma mette a disposizione, accessibile con credenziali individuali;
- la **posta elettronica** istituzionale, utilizzata prevalentemente dagli uffici amministrativi, sia per le comunicazioni in ingresso che in uscita. Anche tutti i docenti dell'Istituto e gli studenti della Scuola Primaria e della Scuola Secondaria di I grado possiedono un account generato dalla scuola per consentire loro l'accesso a piattaforme didattiche e per tutte le attività concordate con i docenti;
- la **piattaforma G-suite**, che con l'insieme delle sue applicazioni e dei suoi servizi web

(Classroom, Groups, Meet, Gmail, Calendar, ecc.) facilita l'archiviazione, il lavoro collaborativo e la didattica condivisa e partecipativa e agevola la comunicazione grazie all'applicazione di metodologie innovative.

In via più informale, sono stati adottati anche altri strumenti di messaggistica istantanea (Whatsapp) sia per comunicazioni interne alla scuola (tra gruppi di docenti, componenti di organi collegiali, di commissioni, ecc.), che per quelle all'esterno verso famiglie e studenti, per facilitare e rendere più partecipata la didattica e la comunicazione con la scuola.

Nelle intenzioni dell'istituzione scolastica c'è quella di dotarsi di un Regolmento sull'utilizzo dei social network, classroom e applicazioni di messaggistica.

3.4 - Strumentazione personale

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

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

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

Come da Regolamento d'Istituto agli studenti è fatto assoluto divieto di usare in autonomia all'interno dell'Istituto scolastico smartphone e/o ogni altro apparato multimediale (walkman, mp3, ipod, ipad, notebook, fotocamera, videocamera, ecc.). Il divieto non si applica soltanto all'orario delle lezioni, ma all'intera permanenza dell'alunno all'interno della struttura scolastica (intervalli, pausa mensa, ecc.). I predetti dispositivi devono essere tenuti spenti e opportunamente custoditi e depositati in borsoni, zaini, giacconi, giammai sul banco né tra le mani.

Le tecnologie digitali e il loro utilizzo in classe non sono interdette del tutto, ma vengono riproposte come strumenti da inserire nella didattica e nelle sperimentazioni laboratoriali. L'uso viene consentito per scopi prettamente didattici, sotto il controllo e la responsabilità del docente che pianifica l'attività didattica. In tal senso, gli smartphone, i tablet e i pc personali possono essere integrati nel lavoro nelle classi quando ben progettato e calibrato per discipline e obiettivi formativi

e didattici e sempre sotto la guida e il controllo dell'insegnante.

Come da Regolamento d'Istituto, ai sensi della C.M. n.362 del 25/08/98, i docenti non possono utilizzare i telefoni cellulari durante l'orario di lavoro per fini personali. L'uso di dispositivi elettronici personali è consentito solo a scopo didattico ed integrativo di quelli scolastici disponibili. Per il personale ATA della scuola: è vietato l'utilizzo di dispositivi elettronici durante l'orario di servizio.

Il nostro Istituto si va aprendo al cosiddetto BOYD (Bring Your Own Device), ossia a politiche per cui l'utilizzo di dispositivi elettronici personali durante le attività didattiche sia possibile ed efficae.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2024/2025).

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti

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

- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

La necessità di sensibilizzare gli studenti ad un utilizzo sicuro e consapevole delle tecnologie digitali, sia in un'ottica di tutela dai rischi potenziali che di valorizzazione delle opportunità esistenti, pone tutta la comunità educante di fronte alla sfida di riconsiderare la propria identità, le proprie risorse e il proprio ruolo educativo.

Il nostro Istituto intende perseguire azioni di prevenzione universale e di sensibilizzazione, attraverso un'efficace integrazione con la rete dei servizi territoriali locali (Polizia postale, ASL, Enti Locali, ecc.), al fine di formare e consolidare quelle competenze educative di base necessarie a poter gestire le situazioni di vita che i ragazzi sperimentano online.

La scuola ha il dovere di creare e mantenere un ambiente sano e sereno nelle classi, per facilitare lo studio e la crescita personale e, insieme con i genitori, ha l'obbligo di aiutare gli alunni a diventare adulti responsabili, in grado di partecipare in modo positivo alla nostra società. Le classi e le amicizie sono le prime piccole "società" nelle quali gli alunni possono fare le loro esperienze e crescere, ma ciò risulta particolarmente difficile quando c'è un ambiente negativo e una dinamica di prevaricazione e sopraffazione.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

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

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

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

Il nostro Istituto condanna severamente ogni atto di cyberbullismo, che ritiene deprecabile e inaccettabile e, come suggerito dalla normativa, si è dotato di un Regolamento di contrasto e prevenzione dei fenomeni di bullismo e cyberbullismo.

Obiettivo di questo regolamento d'Istituto è di affrontare e combattere bullismo e cyberbullismo attraverso azioni di prevenzione, individuazione e riduzione dei comportamenti deviati e violenti, promuovendo anche l'educazione all'uso consapevole della rete internet e delle tecnologie informatiche, al fine di creare un ambiente di apprendimento "sicuro e sereno", in cui tutti gli alunni possano imparare ad accettare e rispettare la "diversità" e poter diventare adulti responsabili e attivi nella società.

La rapida diffusione delle tecnologie, l'espansione della comunicazione elettronica e online e la sua diffusione tra i pre-adolescenti e gli adolescenti hanno determinato l'insorgenza del cyberbullismo, un fenomeno molto pericoloso, esercitato attraverso i social network e gli strumenti comunicativi dei vari dispositivi elettronici (e-mail, sms, chat, blog, siti internet, immagini o video diffusi sulla rete). Si tratta di forme di aggressione e molestie, spesso accompagnate dalla diffusione di messaggi offensivi, foto e immagini denigratorie o dalla creazione di gruppi contro, caratterizzate dall'anonimato e dal fatto che la distanza del persecutore rispetto alla vittima rende più difficile la percezione della sua sofferenza.
L'obiettivo del cyberbullo è sempre quello di molestare la vittima, minacciarla, deriderla, mentre sono richiesti strumenti di contrasto al fenomeno sempre più nuovi ed efficaci.

Gli alunni di oggi, nativi digitali, hanno ottime competenze tecniche ma allo stesso tempo mancano ancora di pensiero riflessivo e critico sull'uso delle nuove tecnologie e di consapevolezza sui rischi del mondo digitale. Il confine tra uso improprio e uso intenzionalmente malevolo della tecnologia, tra incompetenza e premeditazione, è sottile. In questo quadro, la rete ed i social network, possono diventare luoghi dove il bullismo inizia o è mantenuto, per questo motivo la mediazione attiva degli adulti permette l'integrazione di valori e il pensiero critico e aumenta la consapevolezza sui possibili rischi, sulle sfide e le infinite opportunità offerte dal mondo online.

Il fenomeno del cyberbullismo si differenzia dal bullismo tradizionale per la presenza delle seguenti caratteristiche:

- **L'anonimato**: spesso il bullo si nasconde dietro nomi falsi, un nickname, pensando di non poter essere scoperto.
- **Assenza di relazione tra vittima e bullo**: per chi subisce le molestie è ancora più difficile difendersi, perché molto spesso le vittime non riescono neppure a individuare chi è il bullo.
- **Mancanza di feedback emotivo**: il cyberbullo, non vedendo le reazioni della vittima ai suoi comportamenti, non è mai totalmente consapevole del danno che arreca, questo lo rende più disinibito e abbassa i livelli di autocontrollo.
- **Spettatori infiniti**: le persone che possono assistere ad episodi di cyberbullismo sono potenzialmente illimitate, poiché la diffusione in rete è incontrollabile e non avviene con un gruppo di persone definito.

Il fenomeno del cyberbullismo è ancora più grave del bullismo tradizionale perché la tecnologia consente ai bulli di infiltrarsi nelle case e nella vita delle vittime, di materializzarsi in ogni momento,

perché in pochissimo tempo le vittime possono vedere la propria reputazione danneggiata in una comunità molto ampia, poiché i contenuti, una volta pubblicati, possono riapparire a più riprese in luoghi diversi. Spesso i genitori e gli insegnanti ne rimangono a lungo all'oscuro, perché non hanno accesso alla comunicazione in rete degli adolescenti, pertanto può essere necessario molto tempo prima che un caso venga alla luce.

Il problema nelle azioni di contrasto a questi fenomeni è che gli atti di solito avvengono di nascosto e lontano dagli occhi degli adulti (genitori, docenti) e, inoltre, tutti i soggetti coinvolti solitamente provano imbarazzo per quanto subito o visto e preferiscono non parlarne, né a casa, né a scuola. Per questo motivo si rende necessaria una particolare attenzione da parte degli adulti nei confronti del fenomeno e una stretta collaborazione tra scuola e genitori e l'applicazione di regole di comportamento per tutte le classi.

La politica scolastica di antibullismo è da intendersi come una dichiarazione di intenti che guidi l'azione e l'organizzazione all'interno della scuola, l'esplicitazione di una serie di obiettivi concordati che diano agli alunni, al personale e ai genitori un'indicazione e una dimostrazione tangibile dell'impegno della scuola a fare qualcosa contro i comportamenti prevaricatori

Compito dei genitori e della scuola è quello di sostenere i ragazzi e le ragazze, dando loro i giusti consigli e discutendo su quali conseguenze può avere il loro comportamento in rete e ricordando che i bulli e i cyberbulli sono perseguibili penalmente. È opportuno insegnare ai giovani che si possono proteggere dal cyberbullismo trattando i dati privati propri e altrui in modo critico e con la massima sensibilità; fornire indicazioni personali o pubblicare immagini su blog, reti sociali o forum li rende un potenziale bersaglio e da cui ci si può proteggere mantenendo sempre un comportamento rispettoso, evitando di postare dati e informazioni sensibili sul proprio profilo, curare solo amicizie personali e proteggere la sfera privata mediante criteri d'impostazione sicuri.

La tutela della sicurezza dei ragazzi che si connettono alla rete è per la scuola una priorità. Al fine di individuare strategie di prevenzione e di contrasto al cyberbullismo e favorire opportune azioni educative e pedagogiche, la scuola promuove la conoscenza e la diffusione delle regole basilari della comunicazione e del comportamento sul web, come:

- netiquette: un insieme di regole informali che disciplinano il buon comportamento di un utente sul web di Internet, specie nel rapportarsi agli altri utenti;
- norme di uso corretto dei servizi in rete: navigare evitando siti web rischiosi; non compromettere il funzionamento della rete e degli apparecchi che la costituiscono con programmi, virus o malware, costruiti appositamente;
- sensibilizzazione alla lettura attenta delle privacy policy, il documento che descrive nella maniera più dettagliata e chiara possibile le modalità di gestione e il trattamento dei dati personali degli utenti e dei visitatori dei siti internet e dei social network da parte delle aziende stesse;
- costruzione di una propria web-reputation positiva;
- sensibilizzazione sugli effetti psico-fisici del fenomeno dilagante del "vamping" (il restare svegli la notte navigando in rete);
- regolamentazione dell'utilizzo dei telefoni cellulari e di altri dispositivi elettronici a scuola.

4.3 - Hate speech: che cos'è e come prevenirlo

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono quindi un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete. Occorre, in tal senso:

- valorizzare la dimensione relazionale e fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di **hate speech**, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

Inoltre, l'Istituto si potrà avvalere di consulenti/esperti esterni per organizzare incontri formativi rivolti a docenti, genitori ed alunni (Carabinieri, Polizia Postale, equipe Formazione Territoriale del MIUR, associazioni del Territorio preposte allo scopo, ecc.).

4.4 - Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale?

Tale dipendenza, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica, che deve attenzionare il fenomeno e fornire agli studenti gli strumenti affinché siano consapevoli dei rischi che comporta l'iperconnessione.

Il mondo digitale e virtuale, infatti, pur rappresentando un'enorme opportunità di sviluppo e crescita culturale e sociale, nasconde una serie di insidie e pericoli su cui è indispensabile misurarsi, attivando sinergie tra le istituzioni, con l'obiettivo di accrescere il senso della legalità.

La vera sicurezza non sta tanto nell'evitare le situazioni problematiche quanto nell'acquisire gli strumenti necessari per gestirle. Non vanno colpevolizzati gli strumenti e le tecnologie e non va fatta opera repressiva di quest'ultime, occorre viceversa fare opera d'informazione, divulgazione e conoscenza per garantire comportamenti corretti in Rete, intesa quest'ultima come "ambiente di vita" che può dar forma ad esperienze sia di tipo cognitivo che affettive e socio-relazionali.

L'Istituto si propone di promuovere un uso maggiormente consapevole delle tecnologie, per favorire il *benessere digitale*, ossia la capacità di creare e mantenere una relazione sana con la tecnologia. Gli elementi che contribuiscono al benessere digitale sono:

- la ricerca di equilibrio nelle relazioni anche online;
- 'uso degli strumenti digitali per il raggiungimento di obiettivi personali;
- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile;
- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche).

Se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi. È importante non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli studenti, strutturando chiare e semplici regole condivise. Inoltre, sarà fondamentale concordare una linea condivisa con la famiglia, per stabilire mezzi e modalità durante lo studio domestico, con forme di controllo attivo durante la navigazione in Rete.

4.5 - Sexting

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti mediali sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze

impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

Spesso tali immagini o video, anche se inviate ad una stretta cerchia di persone, si diffondono in modo incontrollabile, perchè facilmente modificabili, scaricabili e condivisibili, e possono creare seri problemi, sia personali che legali, alla persona ritratta. L'invio di foto che riguardano minorenni in pose sessualmente esplicite configura, infatti, il reato di distribuzione di materiale pedopornografico.

I contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di "revenge porn", fenomeno che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte. I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro e depressione

---

4.6 - Adescamento online

Il ***grooming*** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di ***teen dating*** (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies – l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

Al fine di prevenire casi di adescamento online è opportuno accompagnare ragazze e ragazzi in un percorso di educazione all'affettività e alla sessualità. Ciò renderebbe gli adolescenti emotivamente più sicuri e pronti ad affrontare eventuali situazioni a rischio, imparando a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri.

È importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore e subentrano vergogna e senso di colpa. Gli adulti coinvolti,

genitori e docenti, devono diventare un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi giudicato, ma compreso e ascoltato. Fondamentale è, quindi, implementare un percorso di educazione digitale che comprenda anche lo sviluppo di capacità relative alla protezione della propria privacy, alla gestione dell'immagine e dell'identità online e alla gestione adeguata delle proprie relazioni online.

Se si sospetta di un caso di adescamento online (o, peggio, se ne dovesse avere certezza) l'adulto di riferimento non deve sostituirsi al minore nell'interlocuzione con l'adescatore. È importante, inoltre, che i dispositivi elettronici della vittima non vengano adoperati per non compromettere eventuali prove, ma cercare di tenere traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video, ecc.).

Casi di adescamento online richiedono l'intervento della Polizia Postale, a cui bisogna rivolgersi con tempestività; questo fenomeno, inoltre, rappresenta una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore, per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (come il Consultorio Familiare, il Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.

4.7 - Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, **concrete o simulate** o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

La legge n. 269 del 3 agosto 1998 *"Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella* ***legge n. 38 del 6 febbraio 2006*** *"Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet"*, segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Secondo la Legge 172/2012 - *Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.*

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione **"Segnala contenuti illegali"** (Hotline).

Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children.

Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia. L'intento è quello di facilitare il processo di rimozione del materiale stesso dalla Rete e allo stesso tempo consentire le opportune attività investigative finalizzate ad identificare chi possiede quel materiale, chi lo diffonde e chi lo produce, ma, soprattutto, ad identificare i minori abusati presenti nelle immagini e video, assicurando la fine di un abuso che potrebbe essere ancora in corso e il supporto necessario.

Parallelamente, per salvaguardare il benessere psicofisico dei minori coinvolti nella visione di questi contenuti, sarà opportuno ricorrere a un supporto psicologico, attraverso una consultazione presso il medico di base o il pediatra di riferimento o rivolgendosi ai servizi socio-sanitari del territorio di appartenenza: Consultori Familiari, Servizi di Neuropsichiatria infantile, centri specializzati sull'abuso e il maltrattamento all'infanzia, ecc.

Se si è a conoscenza di tale tipologia di reato è possibile far riferimento alla:

Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni;

Polizia di Stato – Questura o Commissariato di P.S. del territorio di competenza;

Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza;

Polizia di Stato – Commissariato online.

Studi in materia dimostrano come l'utilizzo di materiale pedopornografico possa essere propedeutico all'abuso sessuale agito ed è quindi fondamentale, in termini preventivi, intervenire per ridurre l'incidenza di tale possibilità. L'abuso sessuale online rappresenta una particolare declinazione dell'abuso sessuale su bambini/e, ragazzi/e, la cui caratteristica fondante è il ruolo ricoperto dalle tecnologie digitali, le quali diventano il mezzo principale attraverso cui l'abuso viene perpetrato, documentato e diffuso in Rete con immagini e/o video. Le dinamiche attraverso cui l'abuso sessuale online si manifesta producono effetti sulle vittime che si aggiungono e moltiplicano

a quelli associati all'abuso sessuale

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2024/2025).

□ Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

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

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

□ Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

I minori potrebbero riferire all'insegnante fatti o eventi personali o altrui, accaduti anche al di fuori della scuola, che potrebbero mettere in allarme il docente. Pertanto sono da considerare degni di segnalazione:

- contenuti afferenti alla violazione della privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);
- contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);
- contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

5.2. - Come segnalare: quali strumenti e a chi

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

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

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

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

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

Strumenti a disposizione di studenti/esse

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

- un indirizzo e-mail specifico per le segnalazioni;

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

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Per quanto riguarda la gestione dei casi, il nostro Istituto ha individuato una figura referente per la prevenzione ed il contrasto del cyberbullismo. La segnalazione del caso dovrà quindi essere fatta al docente referente, il quale si occuperà di raccogliere tutte le informazioni possibili, anche attraverso colloqui di approfondimento con gli attori coinvolti e di riportare l'accaduto al Dirigente. Sarà poi il Dirigente, insieme al docente referente, a valutare se la segnalazione debba essere rivolta ad organi esterni alla scuola, quali la Polizia Postale o i Servizi Sociali, o se il caso possa essere gestito all'interno dell'Istituto stesso e con il coinvolgimento del Consiglio di Classe e delle famiglie degli alunni coinvolti.

Si sceglieranno poi uno o più interventi da attuare a cui seguirà una fase di monitoraggio (cfr. schema di procedura di intervento nell'Allegato 2).

Nei casi di maggiore gravità, si valuterà anche il coinvolgimento di altri attori esterni quali Forze dell'ordine e Servizi sociali.

5.3. - Gli attori sul territorio

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

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

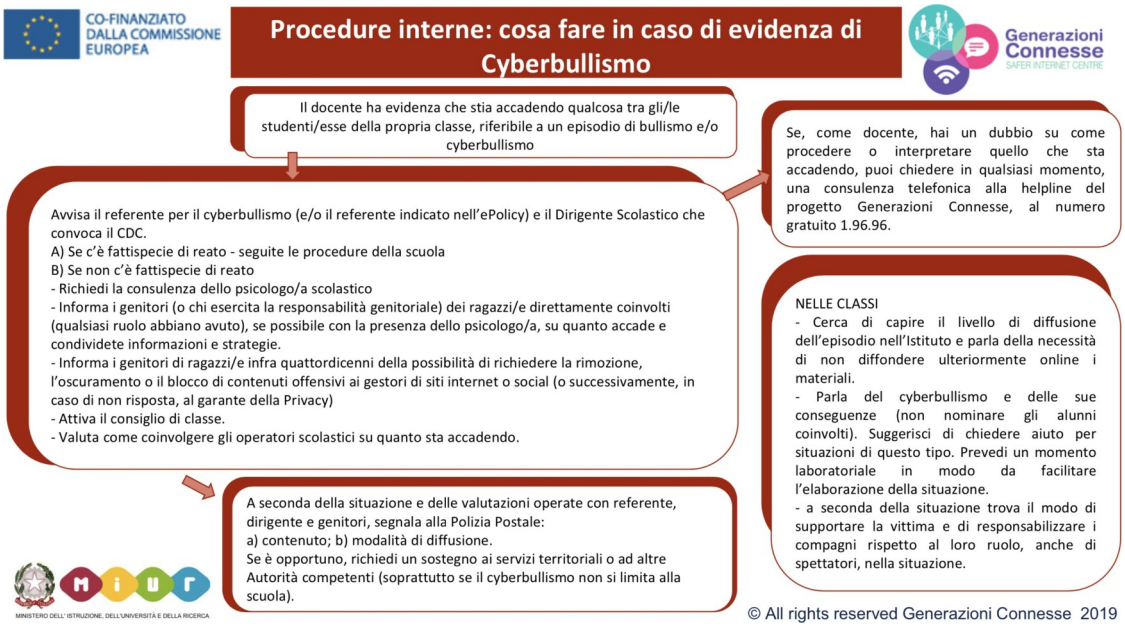
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

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

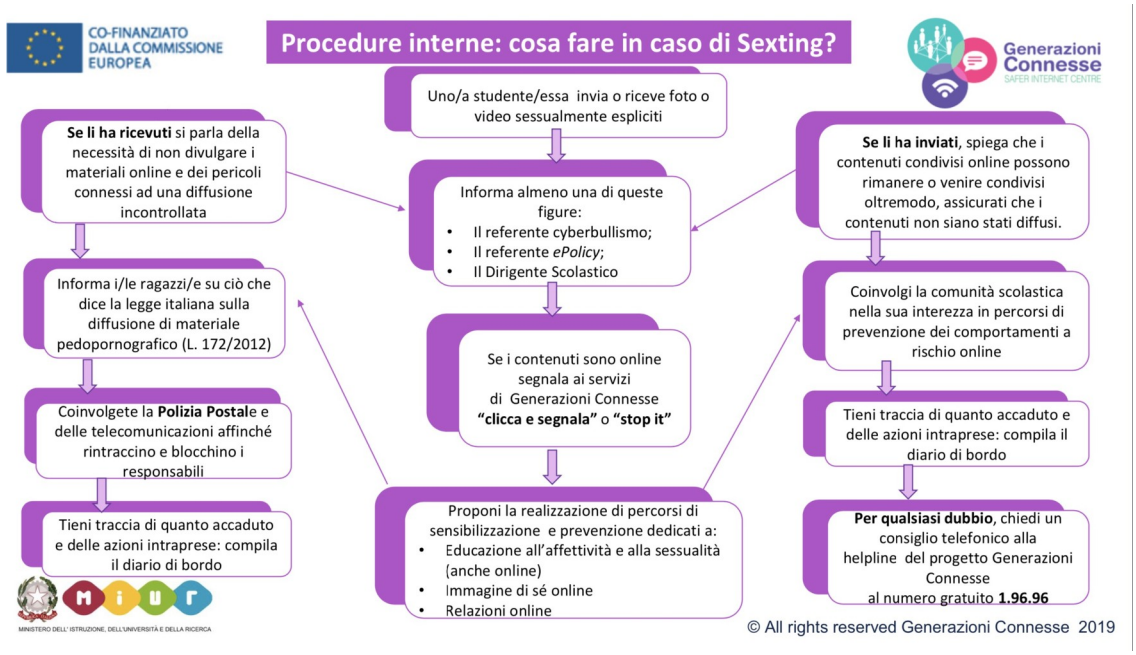
I documenti relativi alle procedure operative e i protocolli sono da elaborare in collaborazione con i suddetti attori del territorio, con cui siglarli unitamente.

5.4. - Allegati con le procedure

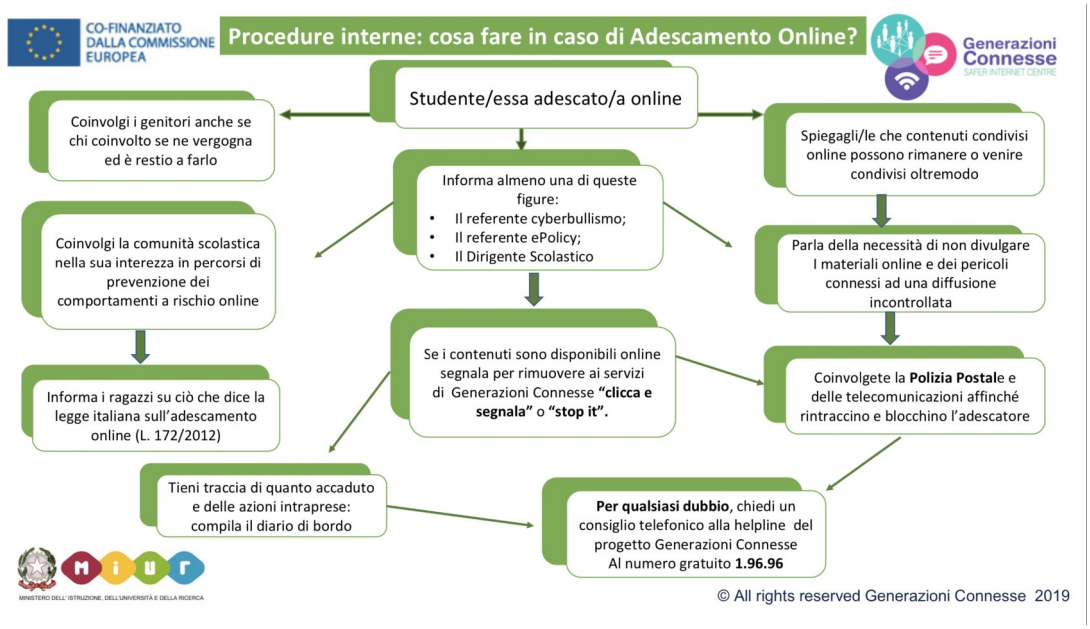
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



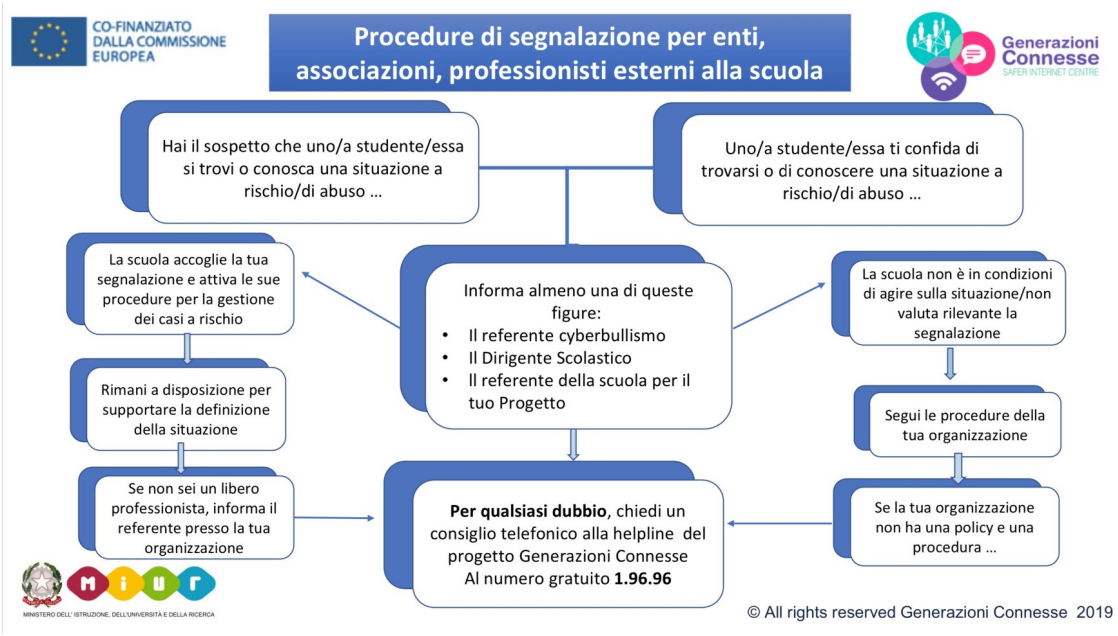
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Istituto Comprensivo Statale "Margherita Hack" * Palermo *

Il Dirigente Scolastico
Dott.ssa Tiziana Dino

Documento firmato digitalmente secondo le indicazioni sulla dematerializzazione, ai sensi e per gli effetti dell'art. 20 comma 2 del d.lgs. 7 marzo 2005, n.82, "Codice dell'Amministrazione Digitale".