Documento di ePolicy

CNIC817008

SOMMARIVA DEL BOSCO

VIA GIANSANA N.37 - 12048 - SOMMARIVA DEL BOSCO - CUNEO

(CN) dott.ssa Anna Giordana

Referenti : Franca Capello, Simona Ingaramo, Manuela Rinaldi

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

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

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.

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.

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).

4 - Condivisione e comunicazione dell'ePolicy all'intera comunità colastica

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

-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica raverso:

pubblicazione del documento sul sito istituzionale della scuola;

Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno olastico;

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

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

5 - Gestione delle infrazioni alla ePolicy

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

6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

Il nostro piano d'azione

Il monitoraggio dell'ePolicy viene pianificato in coerenza con gli obiettivi delineati nella sezione di presentazione del documento, al fine di verificarne l'efficacia, la coerenza con il contesto scolastico e l'aderenza agli obiettivi di promozione della cittadinanza digitale, della sicurezza online e dell'uso consapevole delle tecnologie.

L'implementazione dell'ePolicy sarà oggetto di un monitoraggio continuo, condotto attraverso:

- **Rilevazioni periodiche** (questionari, focus group, osservazioni sul campo) rivolte a docenti, studenti, famiglie e personale ATA, per valutare il grado di conoscenza, applicazione e percezione delle misure previste;
- **Analisi dei dati** raccolti tramite le attività di formazione e sensibilizzazione (numero di partecipanti, feedback, ricadute sulle pratiche didattiche);

- **Monitoraggio delle segnalazioni** di comportamenti scorretti o a rischio in ambiente digitale, attraverso i canali previsti dal sistema di segnalazione interno;
- **Valutazione dei protocolli** e delle procedure attuate per la gestione delle emergenze digitali, verificando il livello di reattività e di coordinamento tra le figure coinvolte.

Il documento sarà aggiornato **con cadenza tiennale**, o in caso di modifiche rilevanti nel contesto scolastico, normativo o tecnologico. L'aggiornamento sarà curato dal **Referente d'Istituto per il bullismo e cyberbullismo** insieme al **Team Digitale**, in raccordo con la **Dirigenza** e il **Collegio Docenti**, garantendo coerenza con quanto previsto nel PTOF e negli altri documenti d'indirizzo dell'istituto.

Tutti gli aggiornamenti saranno comunicati alla comunità scolastica tramite il sito dell'istituto e durante gli incontri di presentazione e restituzione del monitoraggio.

TAB 1. Piano di Azione per l'implementazione e il monitoraggio dell'ePolicy

Obiettivo	**Attività prevista**	**Responsabile/i**	**Tempistica**	**Strumenti di monitoraggio**
Sensibilizzare la comunità scolastica sull'ePolicy	Incontri informativi con docenti, famiglie, studenti (es. durante collegi o assemblee)	Dirigente scolastico dott.ssa Anna Giordana,, Simona Ingaramo (referente ePolicy)	Settembre-Ottobre	Condivisione del documento mediante verbali, brochure, Collegio docenti, Consiglio di Istituto.
Formare il personale scolastico sui temi del digitale sicuro e responsabile	Percorsi di formazione specifici per docenti e ATA (cyberbullismo, privacy, IA, educazione civica, etc.)	Manuela Rinaldi (animatore digitale), Franca Capello (referente bullismo e cyberbullismo, e curricolo di educazione civica)	Svolto a.s. 2023-2024; 2024-2025, fondi PNRR DM 65, DM 66 **Settembre 2025 :** corso sulle competenze orientative con Castoldi Mario	Schede di valutazione dei corsi, questionari di gradimento,relazioni degli esperti e dei tutor
Integrare i principi dell'*ePolicy* nella didattica	Progettazione di UDA su cittadinanza digitale, media education, sicurezza online	Docenti di team/interclasse	Durante l'anno scolastico	Progetti presentati nel PTOF, osservazioni didattiche. creazione di materiale, patentino per lo smartphone.

Attivare un sistema di segnalazione e gestione di criticità digitali	Creazione di un protocollo interno e canali di segnalazione (email, sportello psicologico, sportello bullismo, referente)	Dirigente scolastico dott.ssa Anna Giordana, pro.saFranca Capello (referente bullismo e cyberbullismo e curricolo di educazione civica)	Attivato negli anni scolastici 2023-2024, 2024-2025	Registro delle segnalazioni, esiti e monitoraggio delle azioni
Monitorare la conoscenza e l'applicazione dell'ePolicy	Somministrazione di questionari a studenti, famiglie, docenti	Gruppo di monitoraggio del PTOF (NIV: Ingaramo Simona, Varano Isabella e Brigida Terranova)	Settembre-Ottobre 2025	Analisi dati questionari, *report*
Aggiornare l'ePolicy in base ai dati raccolti	Incontro di revisione e aggiornamento del documento	Simona Ingaramo (referente ePolicy), Team digitale, Referente bullismo, Collegio Docenti	Giugno 2026	Nuova versione pubblicata, verbali di approvazione

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.

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.

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.

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.

Il nostro piano d'azione

TAB 2 Piano di Azione – Formazione e Curricolo

Il presente piano di azione si articola in relazione agli obiettivi indicati nel Capitolo 2 dell'ePolicy, che riguarda la formazione e il curricolo. La scuola si impegna a promuovere lo sviluppo delle competenze digitali degli studenti, a garantire una formazione continua e mirata per il personale docente e a coinvolgere attivamente le famiglie in un percorso educativo condiviso e consapevole.

Ambito	Attività prevista	Responsabile/i	Tempistica	Strumenti di monitoraggio
2.1. Curricolo digitale per studenti	Progettazione e inserimento di attività di cittadinanza digitale, media education, coding, sicurezza online, creazione contenuti digitali nel curricolo	Team docenti, Animatore digitale, Referente ePolicy	Durante l'anno scolastico 2025-2026	UDA e progetti realizzati, osservazioni in classe, relazioni.
2.1. Curricolo digitale per studenti	Utilizzo di strumenti e ambienti digitali (es. GSuite, ambienti di coding, software creativi, escape room, IA,) in attività didattiche trasversali	Docenti disciplinari, Animatore digitale	Durante l'anno scolastico 2025-2026	Osservazioni didattiche, raccolta buone pratiche
2.2. Formazione TIC per i docenti	Organizzazione di corsi su uso integrato e inclusivo delle TIC nella didattica (es. ambienti digitali, strumenti collaborativi, didattica mista)	Animatore digitale, Team digitale	Durante l'anno scolastico 2025-2026	Report presenze, schede di valutazione, relazioni, buone pratiche.
2.3. Formazione su uso sicuro e consapevole delle tecnologie	Incontri con esperti su *cyberbullismo, privacy*, identità digitale, educazione ai *media*	Referente bullismo, Referente *ePolicy,* esperti esterni	Durante l'anno scolastico 2025-2026	*Feedback,* verbali, materiali formativi
2.4. Sensibilizzazione	Incontri informativi con le famiglie,	Dirigente scolastico,	Durante l'anno	Serate, materiali divulgativi, sito web aggiornato

famiglie e aggiornamento Patto	aggiornamento del Patto di corresponsabilità e pubblicazione su sito web	Referente ePolicy, Animatore digitale, Referente bullismo e cyberbullismo	scolastico 2025-2026	

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

3.1 - Protezione dei dati personali

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

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

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

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

di tali dati).

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

In questo paragrafo dell'ePolicy affrontiamo 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.

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.

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.

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.

Il nostro piano d'azione

Finalità

- Promuovere un uso consapevole, innovativo e didattico delle tecnologie installate nei nuovi ambienti digitali.
- Potenziare le competenze digitali di studenti e docenti, in linea con le sfide del mondo contemporaneo.
- Garantire inclusione, equità e sostenibilità nell'accesso e nell'uso delle tecnologie.
- Rafforzare il rispetto delle regole in tema di sicurezza, privacy e cittadinanza digitale**.**

Tab 3.

Obiettivo	**Attività prevista**	**Responsabile /i**	**Tempistica**	**Strumenti di monitoraggio**
Potenziare l'ambiente digitale scolastico in coerenza con i principi dell'ePolicy	Realizzazione di 22 ambienti innovativi PNRR nei tre plessi (aule STEM, musica, sensoriale, web TV…).Tutti i laboratori sono cablati o con rete wifi ed access-point	Dirigente scolastico dott.ssa Anna Giordana, Team digitale, DSGA	Concluso a.s. 2023-2024	Verbali di collaudo, documentazione progettuale, monitoraggio dell'utilizzo
Formare il personale all'uso consapevole e didattico dei nuovi ambienti digitali	Corsi laboratoriali sul campo rivolti ai docenti, con attività pratiche nei nuovi ambienti (STEM, musica, aula sensoriale, web TV). Sono stati attivati i seguenti corsi: -Musica digitale, stanza Snoezeland, Mindfulness, CAA, laboratorio linguistico, educazione civica, fotografia , tinkering ed escape room,	Animatore digitale, Comunità di pratiche, docenti esperti interni ed esterni	a.s. 2024-2025	Schede di valutazione, questionari di gradimento, report delle attività, relazioni di tutor/esperti e della comunità di pratiche tramite l'uso della piattaforma Futura.

Garantire un'infrastruttura digitale sicura e accessibile	Tutti i laboratori sono cablati e dotati di rete internet controllata, conforme alle normative di sicurezza e*Policy*.	Tecnico informatico, DSGA, Animatore digitale, Dirigente scolastico, Team digitale	Permanente	Monitoraggio accessi, report tecnici, audit di sicurezza, registro periodico del materiale e delle infrastrutture.
Regolamentare l'utilizzo degli ambienti innovativi e garantire un uso responsabile	Redazione e diffusione del Regolamento per l'utilizzo dei laboratori innovativi (inserire link: https://drive.google.com/file/d/1lM9EAxVeIaJpuZD2iRoqf498xpRFGHir/view?usp=drive_link)	Dirigente scolastico, Team digitale, Referente ePolicy	a.s. 2024-2025 a.s 2025-2026	Verbali di approvazione, pubblicazione sul sito web, circolari.

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.*

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).

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.

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.

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.

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.

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.

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) o alla polizia postale.

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.

Il nostro piano d'azione

Tab 4.

Obiettivo	Attività prevista	Responsabile/i	Tempistica	Strumenti di monitoraggio
Sensibilizzare la comunità scolastica sull'ePolicy	Incontri informativi con docenti, famiglie, studenti (es. durante collegi o assemblee)	Dirigente scolastico dott.ssa Anna Giordana,, Simona Ingaramo (referente ePolicy)	Settembre-Ottobre	Condivisione del documento mediante verbali, brochure, Collegio docenti, Consiglio di Istituto.
Formare il personale scolastico sui temi del digitale sicuro e responsabile	Percorsi di formazione specifici per docenti e ATA (cyberbullismo, privacy, IA, educazione civica, etc.)	Manuela Rinaldi (animatore digitale), Franca Capello (referente bullismo e cyberbullismo, e curricolo di educazione civica)	Svolto a.s. 2023-2024; 2024-2025, fondi PNRR DM 65, DM 66 **Settembre 2025 :** corso sulle competenze orientative con Castoldi Mario	Schede di valutazione dei corsi, questionari di gradimento,relazioni degli esperti e dei tutor
Integrare i principi dell'*ePolicy* nella didattica	Progettazione di UDA su cittadinanza digitale, media education, sicurezza online	Docenti di team/interclasse	Durante l'anno scolastico	Progetti presentati nel PTOF, osservazioni didattiche. creazione di materiale, patentino per lo smartphone.
Attivare un sistema di segnalazione e gestione di criticità digitali	Creazione di un protocollo interno e canali di segnalazione (email, sportello psicologico, sportello bullismo, referente)	Dirigente scolastico dott.ssa Anna Giordana, pro.saFranca Capello (referente bullismo e cyberbullismo e curricolo di educazione civica)	Attivato negli anni scolastici 2023-2024, 2024-2025	Registro delle segnalazioni, esiti e monitoraggio delle azioni
Monitorare la conoscenza e l'applicazione dell'ePolicy	Somministrazione di questionari a studenti, famiglie, docenti	Gruppo di monitoraggio del PTOF (NIV: Ingaramo Simona, Varano Isabella e Brigida Terranova)	Settembre-Ottobre 2025	Analisi dati questionari, *report*
Aggiornare l'ePolicy in base ai dati raccolti	Incontro di revisione e aggiornamento del documento	Simona Ingaramo (referente ePolicy), Team digitale, Referente bullismo, Collegio Docenti	Giugno 2026	Nuova versione pubblicata, verbali di approvazione

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.

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: sportello.bullismo@istitutogiovanniarpino.edu.it

-sportello di ascolto con professionisti: sportello psicologico

-docenti referente per le segnalazioni: franca.capello@istitutogiovanniarpino.edu.it

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

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.

Il Tribunale per i Minorenni: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.