Documento di ePolicy

SAIS029007

"E. FERRARI"

VIA ROSA IEMMA 301 - 84091 - BATTIPAGLIA - SALERNO (SA)

Daniela Palma

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 daparte 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

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 approccioalla 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).

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.

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.

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.

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 e la revisione del documento E-policy viene affidato al docente Referente ePolicy coadiuvato dal gruppo di lavoro e, ove possibile, con la partecipazione dell'animatore digitale.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.

Azioni da svolgere nei prossimi 3 anni:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori degli alunni dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto agli studenti dell'istituto

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, lavoraree 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.

La formazione del curricolo digitale non può non tener conto di quanto disposto dall'art. 5 della legge 20 agosto 2019 n. 92 (Introduzione dell'insegnamento scolastico dell'educazione civica) interamente dedicato alla "cittadinanza digitale" intesa come capacità di un individuo di avvalersiconsapevolmente e responsabilmente dei mezzi di comunicazione virtuali.

Sono state individuate le seguente aree tematiche:

1° anno: Saper conoscere e saper informarsi.

2° anno: Diritti del cittadino e abusi del web.

3° anno: Big data.

4° anno: Dipendenze e rete.

5° anno: Difesa e protezione dei dati.

Ogni nucleo tematico sarà sviluppato in termini di contenuti, abilità e competenze e acquisizione di

specifici atteggiamenti in capo ai discenti.

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.

In linea con i percorsi individuati nel PDM 2019-2020, tra i quali si annovera quello relativo all'innovazione didattica, il nostro istituto organizza costantemente corsi di formazione per l'utilizzo delle Tic, a beneficio di tutto il corpo docente ricorrendo a figure esperte sia interne che esterne.

L'IISS dell'Erba, dopo una fase di sperimentazione, vanta un buon numero di classi digitali a pieno regime. Tutti i docenti dell'istituto hanno svolto e continuano a svolgere una approfondita attività di formazione per ben utilizzare i dispositivi digitali utilizzati nelle stesse.

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'azioni

AZIONI(da sviluppare nell'arco dell'anno scolastico 2021/2022)

- 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.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzoconsapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo el'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

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

- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggioreinteresse 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.
- Organizzare incontri con esperti per i docenti sulle competenze digitali. Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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 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.

Il nostro istituto si è prontamente adeguato alla suindicata normativa adempiendo a quanto in essa prescritto. E' stata attivata una specifica sezione Privacy sul sito web dell'istituto dove sono state pubblicate tutte le informative e i relativi moduli per l'acquisizione dei consensi, i dati del Dpo, la politica sulla protezione dei dati personali, il vademecum "La scuola a prova di Privacy", organigramma e funzionigramma Privacy, infine si è provveduto a dotarsi del registro dei trattamenti nonché degli accorgimenti tecnici e strutturali idonei al fine di tutelare il diritto alla riservatezza dei componenti la comunità scolastica.

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.
Relativamente agli ambienti di apprendimento il nostro istituto si avvale di

- Tre laboratori di informatica con circa N ° 120 dispositivi digitali.

- 54 LIM,

-una I.C.L. dotata di smart tv e di postazioni mobili che consentono un setting flessibile dell'aula,

152 dispositivi in in comodato gratuito, sui quali vengono scaricati i libri di testo in formato digitale e consentono un'interazione innovativa tra discenti e docenti.

Riguardo agli strumenti di comunicazione esterna, il nostro istituto utilizza il sito web, costantemente aggiornato e i social network (pagina Facebook).

Per la comunicazione interna viene utilizzato

-il registro elettronico che consente di gestire in modo ottimale la comunicazione con le famiglie che hanno la possibilità di essere costantemente informate interagendo direttamente con la scuola

-mail scolastica

-applicativi e piattaforme che hanno favorito un lavoro collaborativo e condiviso rendendo possibile un agevole passaggio alla didattica a distanza nel periodo di lockdown.

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 loroutilizzo 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 istituto si è dotato di una regolamentazione condivisa e specifica su tali aspetti per la quale si rinvia al Regolamento d'Istituto 2020-2021

Il nostro piano d'azioni

AZIONI (da sviluppare nell’arco dell’anno scolastico 2021/2022).

- Effettuare un’analisi sull’utilizzo dei dispositivi personali a scuola da partedegli studenti e delle studentesse
- Effettuare un’analisi sull’utilizzo dei dispositivi personali a scuola da parte deidocenti
- Effettuare un’analisi sull’utilizzo dei dispositivi personali a scuola da parte delpersonale Tecnico Amministrativo e dagli ATA

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

- Organizzare uno o più eventi o attività volti a consultare i docenti dell’Istituto per redigere o integrare indicazioni/regolamenti sull’uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull’uso dei dispositivi digitali personali
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull’uso dei dispositivi digitali 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

Curricolo Digitale d'Istituto

Nel Piano Triennale dell'Offerta Formativa, il curricolo digitale si inserisce come percorso didattico trasversale che coinvolge tutte le discipline d'insegnamento, non soltanto quelle apparentemente più affini, implementando il quadro comune di riferimento europeo DIGCOMP 2.1. (https://www.agid.gov.it/sites/default/files/repository_files/digcomp2-1_ita.pdf).

Il modello DIGCOMP 2.1, elaborato dalla Human Capital and Employment Unit (Joint Research Centre) suincarico del Direttorato Generale Occupazione, Affari Sociali e Inclusione della Commissione Europea e tradotto per l'Italia da AGID (Agenzia per l'Italia Digitale - Presidenza del Consiglio dei Ministri), costituisce un punto di riferimento per le iniziative degli stati membri volte a sviluppare, migliorare e sostenere lo sviluppo delle competenze digitali dei cittadini

Caratteristiche e implementazione del framework DigComp 2.1

Il modello declina la competenza digitale secondo 5 aree e 21 competenze specifiche descritte in termini di conoscenze, abilità e atteggiamenti. Il framework non individua strumenti specifici (che privilegiano l'aspetto tecnologico), ma descrive uno sviluppo completo della competenza digitale che corrisponde ai bisogni di cui sono portatori i cittadini (o futuri cittadini) nell'era digitale: bisogno di essere informato, bisogno di interagire, bisogno di esprimersi, bisogno di protezione dei dati personali, bisogno di gestire situazioni problematiche connesse agli strumenti tecnologici ed ambienti digitali.

Aree	Competenze specifiche
Informazione e alfabetizzazionenella ricerca dei dati	1.1. Navigare, ricercare e filtrare dati, informazioni e contenuti digitali. 1.2. Valutare dati, informazioni e contenuti digitali. 1.3. Gestire dati, informazioni e contenuti digitali.
Comunicazione eCollaborazione	2.1. Interagire tramite le tecnologie digitali. 2.2. Condividere tramite le tecnologie digitali. 2.3. Sviluppare le competenze di cittadinanza tramite le tecnologie digitali. 2.4. Sviluppare forme di collaborazione tramite le tecnologie digitali 2.5. Netiquette 2.6. Gestire l'identità digitale
Creazione di contenuti digitali	3.1. Sviluppare contenuti digitali. 3.2. Integrare e rielaborare contenuti digitali 3.3. Copyright e licenze 3.4. Programmazione
Sicurezza	4.1. Proteggere i dispositivi 4.2. Proteggere i dati personali e la privacy4.3.Tutelare la salute e il benessere 4.4. Proteggere l'ambiente
Problem Solving	5.1. Risolvere i problemi tecnici 5.2. Identificare i bisogni e le soluzioni tecnologici 5.3.Utilizzare le tecnologie digitali in modo creativo 5.4. Identificare gli squilibri nelle competenze digitali

Il modello DigComp 2.1 definisce 8 livelli di padronanza per lo sviluppo delle competenze, riassunte nella seguente griglia di riferimento riepilogativa, attraverso risultati di apprendimento (declinati in termini di verbi di azione secondo la tassonomia di Bloom) guidati dalla struttura e dal vocabolario del quadro europeo delle qualifiche EQF (European Qualification Framework)

Livelli di competenza DigComp 1.0	Livelli di competenza DigComp 2.1	Complessità del compito	Autonomia	Dominio cognitivo
Base	1	Compiti semplici	Con guida	Conoscere
	2	Compiti semplici	In autonomia e con guida dove necessario	Conoscere
Intermedio	3	Compiti ben definiti e di routine e semplici problemi	Da solo/a	Comprendere
	4	Compiti e problemi ben definiti e non routinari	In modo indipendente e secondo i miei bisogni	Comprendere
Avanzato	5	Differenti compiti e problemi	Guidando altri	Applicare
	6	Compiti specifici	Abile ad adattarsi ad altri in un contesto complesso	Valutare
Altamente specializzato	7	Problemi complessi con soluzioni limitate	In grado di integrarsi per contribuire alla pratica professionale e guidare altri	Creare
	8	Problemi complessi con diversi fattori di interazione	In grado di proporre nuove idee e processi nel settore	Creare

Nel Curricolo Digitale d'Istituto, la progressione dei livelli di padronanza delle competenze e l'acquisizione dei risultati di apprendimento non segue una linea rigidamente definita, ma una progettazione vocazionalmente ispirata alla personalizzazione dei percorsi d'apprendimento declinati, attraverso le Unità d'Apprendimento, nel Progetto Formativo Individualizzato.

Lo stesso modello DigiComp 2.1, a cui ci si richiama, fornisce una serie di esempi, non esaustiva, per la definizione dei compiti di realtà cui gli studenti sono chiamati per esercitare la competenza consentendo la sua valutazione e certificazione.

Rubriche di valutazione delle competenze digitali

La descrizione dei livelli di padronanza della competenza digitale, in termini di risultati d'apprendimento, sono tratti dal documento di riferimento DigComp 2.1 e costituiscono la base per orientare progettazione didattica, valutazione e certificazione delle competenze. Le rubriche si riferiscono alla declinazione curricolare delle competenze digitali e, pertanto, saranno oggetto di annuale revisione e integrazione da parte dei Dipartimenti disciplinari ed approvazione del Collegio dei docenti.

Per ogni competenza specifica, sono riportati i descrittori (intesi come traguardi d'apprendimento) riferiti in particolare ai livelli ***Base***, ***Intermedio*** ed ***Avanzato*** in accordo con il modello di certificazione delle competenze di base attese all'assolvimento dell'obbligo di istruzione (DM 9/2010) ed al modello dicertificazione delle competenze in uscita dal 1° Ciclo d'Istruzione (DM 742/2017).

Nelle seguenti Rubriche, il livello ***Iniziale*** (caratterizzato da un raggiungimento non completo dei traguardi del livello ***Base***) ed il livello ***Altamente Specializzato*** (caratterizzato da una maggiore creatività ed autonomia rispetto al livello ***Avanzato***) non sono riportati per semplificarne lettura ed applicazione.

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

Area 1 - Informazionee alfabetizzazione nella ricerca dei dati			
Competenza	**Livelli**		
	Base	**Intermedio**	**Avanzato**
1.1. Navigare, ricercare e filtrare dati, informazioni e contenuti digitali.	• individuare i miei fabbisogniinformativi, • trovare dati, informazioni e contenuti attraverso una semplice ricerca in ambienti digitali, •scoprire come accedere a questi dati, informazioni e contenuti e navigare al loro interno, • identificare semplici strategiedi ricerca personali.	• spiegare i miei fabbisogni informativi, • svolgere ricerche ben definite e sistematiche per individuare informazioni e contenuti negli ambienti digitali, • spiegare come accedervi e navigare al loro interno. • spiegare strategie personali di ricerca ben definite e sistematiche.	• rispondere ai fabbisogni informativi, • applicare ricerche per ottenere dati, informazioni e contenuti in ambienti digitali, • mostrare come accedere a questi dati, informazioni e contenuti e navigare al loro interno, • proporre strategie di ricerca personali.
1.2. Valutare dati,informazioni e contenutidigitali.	• rilevare la credibilità e l'affidabilità delle fonti comuni di dati, informazioni e contenuti digitali.	• eseguire l'analisi, il confronto e la valutazione della credibilità edell'affidabilità di fonti ben definite di dati, informazioni e contenuti digitali, • eseguire l'analisi, l'interpretazione e la valutazione di dati, informazioni e contenutidigitali ben definiti.	• svolgere una valutazione della credibilità e dell'affidabilità di fonti diversedi dati, informazioni e contenuti digitali, • svolgere una valutazione di dati, informazioni e contenuti digitali diversi.
1.3. Gestire dati, informazionie contenuti digitali.	• individuare come organizzare, archiviare e recuperare con facilità dati, informazioni e contenuti negli ambienti digitali. • riconoscere dove organizzarli in modo semplice in un ambiente strutturato.	• selezionare, dati, informazioni e contenuti allo scopo di organizzarli, archiviarli e recuperarli in maniera sistematica all'interno di ambienti digitali. • organizzarli in modo sistematico in un ambiente strutturato.	• manipolare informazioni, datie contenuti per facilitarnel'organizzazione, l'archiviazione e il recupero. • organizzarli ed elaborarli inun ambiente strutturato. adeguare la gestione diinformazioni, dati e contenutiaffinché vengano recuperati earchiviati nel modo più facile eopportuno. • adeguarli affinché vengano organizzati ed elaborati nell'ambiente strutturato più adatto

5

Area 2 - Comunicazione eCollaborazione			
Competenza	**Livelli**		
	Base	**Intermedio**	**Avanzato**
2.1. Interagire tramite le tecnologie digitali.	• scegliere tecnologie digitali semplici per l'interazione, e • identificare adeguati mezzi di comunicazione semplici per undeterminato contesto.	• interagire con le tecnologie digitali in modo ben definito e sistematico, e • scegliere mezzi di comunicazione digitali ben definiti e di routine per un determinato contesto.	• utilizzare svariate tecnologie digitali per l'interazione, • mostrare agli altri i mezzi di comunicazione digitali più appropriati per un determinato contesto. • adeguare i mezzi di comunicazione più appropriati per un determinato contesto.
2.2. Condividere tramite le tecnologie digitali.	• riconoscere semplicitecnologie digitali appropriate	• scegliere tecnologie digitaliappropriate, ben definite e	• condividere dati,informazioni e contenuti

	per condividere dati, informazioni e contenuti digitali. • individuare prassi semplici diriferimento e attribuzione.	sistematiche per condividere dati, informazioni e contenuti digitali. • spiegare come agire da intermediari per condividere informazioni e contenuti attraverso tecnologie digitali ben definite e sistematiche. • illustrare prassi di riferimento e attribuzione ben definite e sistematiche..	digitali attraverso una varietà di appropriati tool digitali • mostrare ad altri come agire da intermediari per condividere informazioni e contenuti attraverso tecnologie digitali • applicare diverse prassi di riferimento e attribuzione.
2.3. Sviluppare le competenzedi cittadinanza tramite le tecnologie digitali.	• individuare semplici servizi digitali per partecipare allavita sociale. • riconoscere semplici tecnologie digitali appropriate per potenziare le mie capacità personali e professionali e partecipare come cittadino alla vita sociale.	• scegliere semplici servizi digitali ben definiti e sistematici per partecipare alla vita sociale. • indicare tecnologie digitali appropriate ben definite e sistematiche per potenziare le mie capacità personali e professionali e partecipare come cittadino alla vita sociale.	• proporre servizi digitali diversi per partecipare alla vitasociale. • utilizzare tecnologie digitali appropriate per potenziare le mie capacità personali e professionali e partecipare come cittadino alla vitasociale.
2.4. Sviluppare forme di collaborazione tramite le tecnologie digitali	• scegliere strumenti e tecnologie digitali semplici peri processi collaborativi.	• scegliere strumenti digitali e tecnologie ben definiti e sistematici per i processi collaborativi	• variare l'utilizzo degli strumenti e delle tecnologie digitali più appropriati per i processi collaborativi. • scegliere gli strumenti e le tecnologie digitali più appropriati per co-costruire e co-creare dati, risorse e know- how.
2.5. Netiquette	• distinguere le semplici norme comportamentali e il know- how per l'utilizzo delle tecnologie digitali e l'interazione con gli ambienti digitali. • scegliere modalità di comunicazione e strategie semplici adattate a un pubblico • distinguere le differenze culturali e generazionali semplici di cui tener conto negli ambienti digitali	• chiarire norme comportamentali e know-how ben definiti e sistematici per l'utilizzo delle tecnologie digitali e l'interazione con gli ambienti digitali. • esprimere strategie di comunicazione ben definite e sistematiche adattate a un pubblico • descrivere differenze culturali e generazionali ben definite e sistematiche di cui tener conto negli ambienti digitali.	• applicare norme comportamentali e know-howdiversi nell'utilizzo delle tecnologie digitali e nell'interazione con gli ambienti digitali. • applicare strategie di comunicazione diverse negli ambienti digitali adattate a un pubblico • applicare differenze culturali e generazionali diverse di cui tener conto negli ambienti digitali.
2.6. Gestire l'identità digitale	• individuare un'identità digitale, • descrivere modi semplici di proteggere la mia reputazione online, • riconoscere dati semplici che produco attraverso strumenti,ambienti o servizi digitali.	• distinguere tra una serie di identità digitali ben definite e sistematiche, • spiegare modalità ben definite e sistematiche per tutelare la mia reputazione online, • descrivere dati ben definiti che produco in modo sistematico attraverso strumenti, ambienti o servizi digitali.	• utilizzare una varietà di identità digitali, • applicare diverse modalità per proteggere la mia reputazione online, • utilizzare i dati che produco attraverso numerosi strumenti, ambienti o servizi digitali.

Area 3 - Creazione dicontenuti digitali			
Competenza	**Livelli**		
	Base	**Intermedio**	**Avanzato**
3.1. Sviluppare contenutidigitali.	• individuare modalità per creare e modificare contenuti semplici in formati semplici, • scegliere come esprimermi attraverso la creazione di strumenti digitali semplici	• indicare modalità per crearee modificare contenuti ben definiti e sistematici in formati ben definiti e sistematici, • esprimermi attraverso la creazione di strumenti digitali ben definiti e sistematici.	• applicare modi per creare e modificare i contenuti in diversi formati, • mostrare modalità per esprimermi attraverso la creazione di strumenti digitali.

3.2. Integrare e rielaborare contenuti digitali	• scegliere modi per modificare, affinare, migliorare e integrare voci semplici di nuovi contenuti e informazioni per crearne di nuovi e originali.	• spiegare modi per modificare, affinare, migliorare e integrare voci bendefinite di nuovi contenuti e informazioni per crearne di nuovi e originali	• lavorare con contenuti e informazioni nuovi e diversi, modificandoli, affinandoli, migliorandoli e integrandoli per crearne di nuovi e originali.
3.3. Copyright e licenze	• individuare semplici regole di copyright e licenze da applicare a dati, informazioni digitali e contenuti.	• individuare regole di copyright e licenze ben definite e sistematiche da applicare a dati, informazioni digitali e contenuti.	• adottare diverse regole di copyright e licenze da applicare a dati, informazioni digitali e contenuti.
3.4. Programmazione	• elencare semplici istruzioni per un sistema informatico per risolvere un semplice problema o svolgere un compito semplice.	• elencare istruzioni ben definite e sistematiche per un sistema informatico per risolvere problemi sistematicio svolgere compiti sistematici.	• operare con istruzioni per un sistema informatico per risolvere un problema diverso o svolgere compiti diversi.

Area 4 - Sicurezza			
Competenza	**Livelli**		
	Base	**Intermedio**	**Avanzato**
4.1. Proteggere i dispositivi	• individuare semplici modalità per proteggere i miei dispositivi e contenuti digitali • distinguere semplici rischi e minacce negli ambienti digitali, • scegliere semplici misure di sicurezza, • individuare semplici modalità per tenere conto dell'affidabilità e della privacy	• individuare modi ben definiti e sistematici per proteggere i miei dispositivi e contenutidigitali • distinguere rischi e minacce ben definiti e sistematici negli ambienti digitali, • scegliere misure di sicurezza ben definite e sistematiche. • individuare modi ben definiti e sistematici per tenere in debita considerazioneaffidabilità e privacy	• applicare differenti modalità per proteggere i dispositivi e i contenuti digitali • distinguere una varietà di rischi e minacce negli ambientidigitali, • applicare misure di sicurezza, • individuare varie modalità per tenere in debita considerazione l'affidabilità e la privacy
4.2. Proteggere i datipersonali e la privacy	• scegliere semplici modalità per proteggere i miei dati personali e la privacy negli ambienti digitali • individuare semplici modalità per utilizzare e condividere informazioni personali proteggendo me stesso e gli altri da danni. • individuare semplici clausole della politica sulla privacy su come vengono utilizzati i dati personali nei servizi digitali.	• spiegare modalità ben definite e sistematiche per proteggere i miei dati personali e la privacy negli ambienti digitali • spiegare modalità ben definite e sistematiche per utilizzare e condividere informazioni personali proteggendo me stesso e gli altri da danni. • individuare clausole ben definite e sistematiche della politica sulla privacy su come vengono utilizzati i dati personali nei servizi digital	• applicare modalità diverse per proteggere i miei dati personali e la privacy negli ambienti digitali • applicare modalità specifiche diverse per condividere i miei dati proteggendo me stesso e gli altri da pericoli. • spiegare le clausole della politica sulla privacy inerenti le modalità di utilizzo dei dati personali nei servizi digitali.
4.3.Tutelare la salute e il benessere	• distinguere semplici modalità per evitare rischi per la salute e minacce al benessere psico- fisico quando si utilizzano le tecnologie digitali, • scegliere semplici modalità per proteggermi da possibili pericoli negli ambienti digitali, • individuare semplici tecnologie digitali per il benessere sociale el'inclusione sociale.	• spiegare modalità ben definite e sistematiche per evitare rischi per la salute e minacce al benessere psico-fisico quando si utilizzano le tecnologie digitali, • scegliere modalità ben definite e sistematiche per proteggermi da possibili pericoli negli ambienti digitali, • indicare tecnologie digitali ben definite e sistematiche per il benessere sociale e l'inclusione sociale.	• mostrare diverse modalità perevitare rischi per la salute e minacce al benessere psico-fisico quando si utilizzano le tecnologie digitali, • applicare diverse modalità per proteggere me stesso e gli altri da pericoli negli ambienti digitali, • mostrare diverse tecnologie digitali per il benessere sociale e l'inclusione sociale.

4.4. Proteggere l'ambiente	• riconoscere semplici impatti ambientali delle tecnologie digitali e il loro utilizzo.	• indicare impatti ambientali ben definiti e sistematici delle tecnologie digitali e il loro utilizzo	• scegliere le soluzioni più appropriate per proteggere l'ambiente dall'impatto delle tecnologie digitali e del loro utilizzo.

Area 5 - Problem Solving			
Competenza	**Livelli**		
	Base	**Intermedio**	**Avanzato**
5.1. Risolvere i problemi tecnici	• individuare semplici problemi tecnici nell'utilizzo dei dispositivi e delle tecnologie digitali • identificare semplici soluzioni per risolverli	• indicare problemi tecnici ben definiti e sistematici nell'utilizzo dei dispositivi e degli ambienti digitali • scegliere soluzioni ben definite e sistematiche per questi problemi.	• valutare i problemi tecnici derivanti dall'utilizzo degli ambienti digitali e dei dispositivi, • applicare diverse soluzioni a questi problem
5.2. Identificare i bisogni e lesoluzioni tecnologici	• individuare esigenze e riconoscere semplici strumenti digitali e possibili risposte tecnologiche per soddisfarli, • scegliere semplici modalità per adattare e personalizzare gli ambienti digitali alle esigenze personali.	• indicare esigenze ben definite e sistematiche, • scegliere strumenti digitali ben definiti e sistematici e possibili risposte tecnologiche per soddisfarli. • scegliere modalità semplici eben definite per adattare e personalizzare gli ambienti digitali alle esigenze personali	• valutare le esigenze e applicare diversi strumenti digitali e possibili risposte tecnologiche per soddisfarli, • utilizzare diverse modalità per adattare e personalizzare gli ambienti digitali alle esigenze personali.
5.3.Utilizzare le tecnologie digitali in modo creativo	• individuare semplici strumenti e tecnologie digitali per creare know-how e innovare processi e prodotti. • dimostrare interesse a livello individuale e collettivo nei processi cognitivi semplici per comprendere e risolvere problemi concettuali e situazioni problematiche negli ambienti digitali	• scegliere strumenti e tecnologie digitali da utilizzare per creare know-how ben definito e processi e prodotti innovativi ben definiti. • partecipare individualmente e collettivamente ad alcuni processi cognitivi per comprendere e risolvere problemi concettuali ben definiti e sistematici e situazioni problematiche negli ambienti digitali.	• applicare diversi strumenti e tecnologie digitali per creare know-how e processi e prodotti innovativi. • applicare individualmente e collettivamente processi cognitivi per risolvere diversi problemi concettuali e situazioni problematiche negli ambienti digitali.
5.4. Identificare gli squilibri nelle competenze digitali	• riconoscere gli aspetti da migliorare o aggiornare per i miei fabbisogni di competenzedigitali. • individuare dove cercare opportunità di crescita personale e tenermi al passo con l'evoluzione digitale.	• spiegare gli aspetti da migliorare o aggiornare per i miei fabbisogni di competenzedigitali. • indicare dove cercare opportunità di crescita personale ben definite e tenermi al passo con l'evoluzione digitale.	• dimostrare gli aspetti da migliorare o aggiornare per i miei fabbisogni di competenze digitali. • illustrare modalità diverse per supportare gli altri nello sviluppo delle loro competenzedigitali. • proporre diverse opportunità di crescita personale trovate e tenersi al passo con l'evoluzione digitale.

5

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 siaquello 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.

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

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 incontatto 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 lealtre 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.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021).

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzosicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associatiall'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti
- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- 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).

- Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.
- 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.
- Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.
- Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.
- Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online nella scuola

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 modalitàattraverso 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.

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 preparazionee 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.

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.

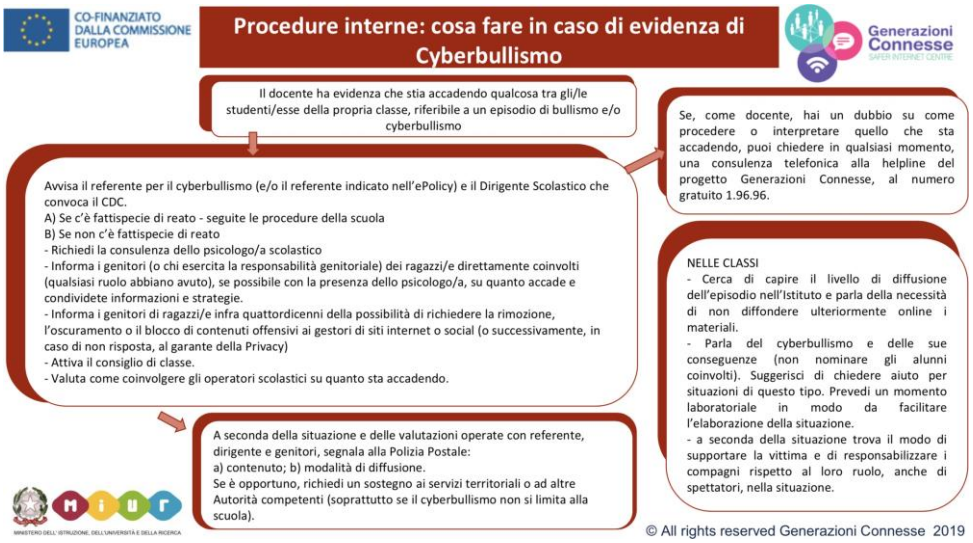
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **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 casidi violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.

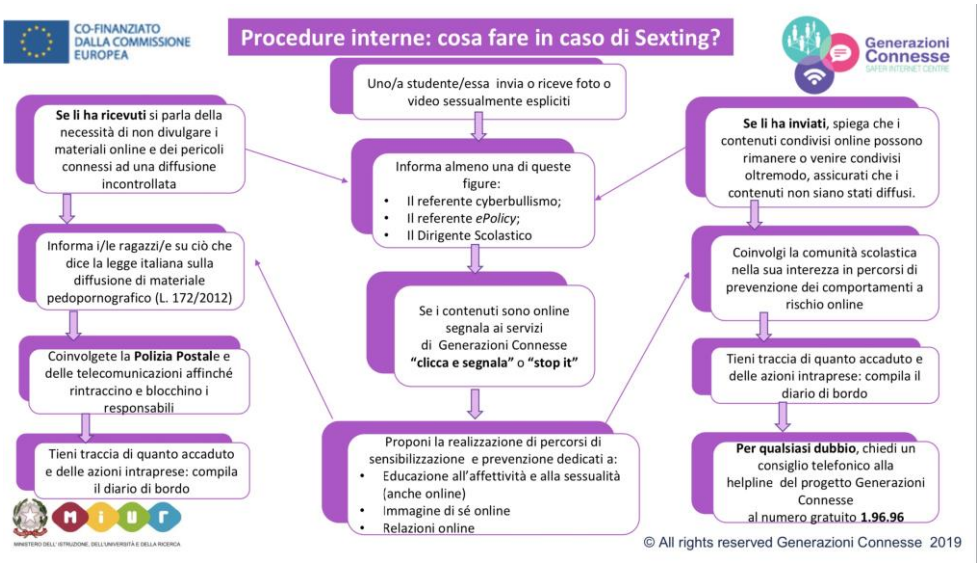
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

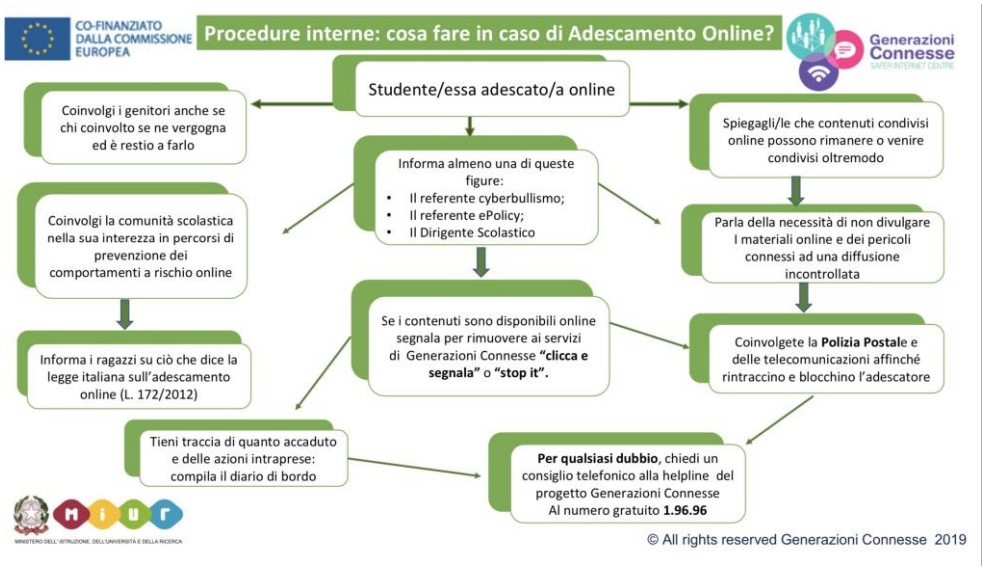
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



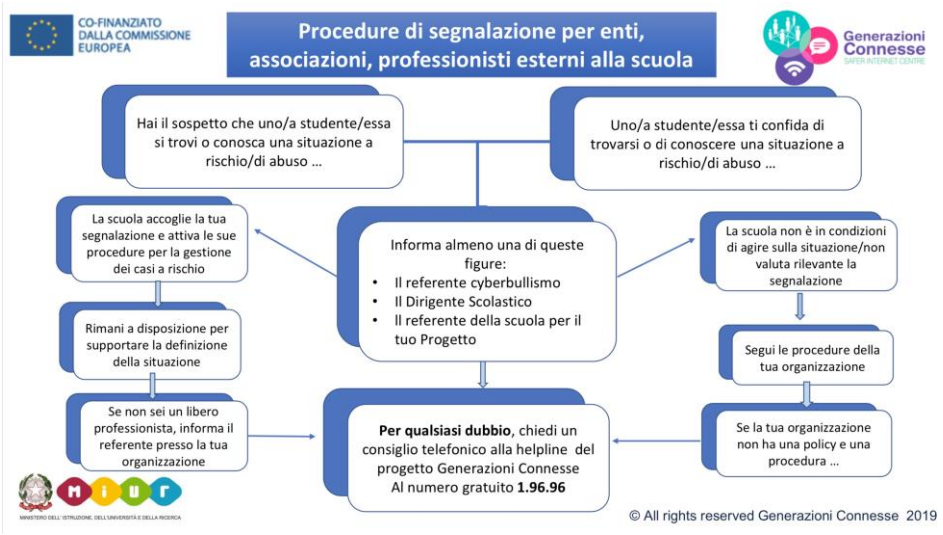
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

- Scheda di segnalazione
- Diario di bordo
- iGloss@ 1.0 l'ABC dei comportamenti devianti online
- Elenco reati procedibili d'ufficio

Il nostro piano d'azioni

Sulla base delle Linee Guida per l'uso positivo delle tecnologie digitali e della prevenzione dei rischi nelle scuole, vengono assunti i seguenti punti quali indicatori di co-costruzione tra scuola-famiglia-servizi territoriali, al fine di creare un modello composito e lineare di azioni condivise:

- coinvolgimento di tutti gli attori della scuola: studenti e studentesse, docenti, genitori e personale ATA, per la realizzazione di una autentica comunità educante;

- alleanza educativa tra scuola e famiglia;

- interventi educativi ed azioni di supporto, quale prevenzione per eventuali comportamenti a rischio;

- misure preventive specifiche di tutela anche con l'ausilio di attori territoriali, come forze dell'ordine ed ASP per servizi specialistici;

- promozione dell'educazione al rispetto;

- sviluppo del pensiero critico;

- promozione dell'Educazione Civica Digitale.