Documento di ePolicy

BATD02000A

ISTITUTO TECNICO ECONOMICO "F. M. GENCO"

PIAZZA LAUDATI 1 - 70022 - ALTAMURA - BARI (BA)

Leonardo Campanale

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

Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

L'Istituto Tecnico Economico Statale "Francesco Maria Genco", in conformità con "Le linee di orientamento per la prevenzione e il contrasto al bullismo e cyberbullismo", emanate
dal Miur ad ottobre del 2017, ha elaborato il documento E-policy in modo da dotare la scuola di procedure, norme comportamentali e attività che servano ad educare e sensibilizzare tutta la comunità educante ai problemi legati ad un uso improprio delle tecnologie digitali e di Internet. I docenti, il personale Ata, i genitori devono garantire che gli studenti siano in grado di utilizzare le tecnologie digitali in modo sicuro.
E' necessario avviare una politica di sicurezza della navigazione on line volta ad un controllo dell'uso delle strumentazioni digitali e alla diffusione di buone pratiche di comunicazione sui social network. Dotare la scuola di una propria E-policy, a integrazione del Regolamento d'Istituto, è necessario per avere chiare quali siano le azioni da attivare per gestire le infrazioni e quali azioni sanzionatorie vengano previste a seconda della gravità dell'evento
verificatosi.
Nello specifico, è un documento programmatico autoprodotto dalla scuola volto a descrivere:

- il proprio approccio alle tematiche legate alle competenze digitali, alla privacy e alla sicurezza online e ad un uso positivo delle tecnologie digitali nella didattica;
- le norme comportamentali e le procedure per l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione;
- le misure per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

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.

La scuola definisce in maniera chiara i ruoli, i compiti e le responsabilità degli attori

del percorso formativo volto alla promozione di un uso consapevole della Rete e delle Tic.

Il Dirigente scolastico deve:

- provvedere alla formazione e all'aggiornamento personale
- garantire la formazione del personale scolastico al fine di diffondere norme finalizzate ad un uso corretto di Internet
- garantire percorsi formativi rivolti ai docenti sull'utilizzo delle Tic nella didattica
- garantire l'integrazione delle modalità di un utilizzo corretto delle Tic e della Rete nel curriculum di studio
- garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza online
- seguire le procedure previste in caso di attribuzione di responsabilità al personale scolastico, in caso di incidenti occorsi agli studenti e alle studentesse nell'utilizzo delle Tic a scuola

L'Animatore Digitale con il supporto del team digitale:

- fornisce consulenza e informazioni al personale in relazione ai rischi online e alle misure di prevenzione e gestione degli stessi
- stimola la formazione interna all'istituzione al fine di sviluppare una cultura della scuola digitale
- rileva le problematiche che si potrebbero verificare in seguito ad un uso improprio delle Tic e della Rete assicura che gli utenti possano accedere alla rete della scuola solo tramite password
- cura il sito web della scuola
- coinvolge la comunità scolastica nella partecipazione ad attività attinenti alla scuola digitale
- individua e propone soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola

Il referente del bullismo e cyberbullismo deve:

- coordinare e promuovere iniziative finalizzate alla prevenzione e al contrasto del fenomeno del bullismo e del cyberbullismo
- collaborare con le Forze di Polizia, associazioni del territorio per organizzare progetti e percorsi formativi rivolti ai docenti, ai genitori e agli studenti

Il Direttore dei servizi generali e amministrativi deve:

- assicurare che l'infrastruttura tecnica della scuola sia sottoposta a continua manutenzione da parte di tecnici in modo che sia sicura e non esposta ad attacchi dannosi esterni
- garantire che i canali di comunicazione all'interno della scuola e fra scuola e

famiglia funzionino efficacemente per le notifiche e le informazioni da parte del Dirigente Scolastico e dell'Animatore Digitale relative ad un uso corretto delle Tic e di Internet

I Docenti devono:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di Internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di Internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantire che gli alunni comprendano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di Internet;
- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete, ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo all'Animatore Digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- segnalare al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di Internet per l'adozione delle procedure previste dalla normativa.

Il Personale Ata deve:

- partecipare ad attività di formazione sul tema del bullismo e del cyberbullismo
- segnalare comportamenti non adeguati e/o episodi di bullismo

Gli studenti devono:

- utilizzare in maniera responsabile le tecnologie digitali durante le attività didattiche in conformità con quanto richiesto dai docenti
- comprendere le opportunità offerte dalle tecnologie digitali e dalla Rete per la ricerca di contenuti e informazioni sempre nel rispetto delle norme derivanti dai diritti d'autore
- usare la comunicazione in Rete nel rispetto della privacy altrui
- comprendere l'importanza di adottare sistemi per la sicurezza online e non correre rischi
- partecipare attivamente ad eventi, progetti ed attività sul tema dei rischi online e alle modalità di tutela contro attacchi di bullismo e/o cyberbullismo e sulla gestione delle emozioni e relazioni con i pari.

I Genitori devono:

- partecipare ad iniziative legate all'uso responsabile delle tecnologie digitali e della Rete
- condividere con i docenti le linee educative relative all'uso corretto delle Tic e di Internet nella didattica
- controllare che i propri figli usino correttamente la rete e le tecnologie digital segnalare ai docenti eventuali comportamenti dei propri figli legati ad un uso improprio della Rete e delle tecnologie digitali
- accettare e sottoscrivere il documento E-policy adottato dall'Istituto Infine, gli Enti esterni e le Associazioni devono:
- conformarsi alla politica della scuola riguardo l'uso consapevole delle TIC e della Rete;
- promuovere comportamenti sicuri,
- promuovere la sicurezza online
- assicurare la protezione degli studenti durante le attività proposte.

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

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

Gli esperti o associazioni esterne alla scuola devono segnalare al Dirigente scolastico, al Referente del bullismo o al coordinatore di classe, eventuali episodi di bullismo e cyberbullismo da parte degli studenti e delle studentesse.
È importante garantire che tutti i soggetti esterni che erogano attività in ambito scolastico siano sensibilizzati e resi consapevoli dei rischi online che possono correre gli studenti e le studentesse e dei comportamenti corretti che devono adottare a scuola.
L'Istituto si riserva di richiedere agli attori esterni, eventualmente, il casellario giudiziale come fattore ulteriormente protettivo verso i minori. L'obiettivo è quello di verificare l'esistenza (o meno) di condanne per alcuni reati previsti dal Codice penale e nello specifico gli articoli 600-bis (prostituzione minorile), 600-ter (pornografia minorile), 600-quater (detenzione di materiale pornografico), 600-quinquies (iniziative turistiche volte allo sfruttamento della prostituzione minorile), 609-undecies (adescamento di minorenni), o l'irrogazione di sanzioni interdittive all'esercizio di attività che comportino contatti diretti e regolari con i minori.

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

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

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

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

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

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

Il documento E-policy è un documento condiviso da tutte le componenti che operano nella scuola: personale scolastico e genitori.
Gli studenti

- saranno istruiti riguardo all'uso responsabile di Internet prima di poter accedere alla rete
- saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione;
- l'elenco delle regole per la sicurezza on-line sarà pubblicato in tutte le aule o laboratori con accesso a Internet;

Il personale scolastico:
Il presente documento E-policy, adottato dall'Istituto, fornisce la linea di condotta da seguire in materia di sicurezza nell'utilizzo delle tecnologie digitali e di Internet. Essa viene condivisa da tutti gli attori del percorso educativo degli studenti e delle studentesse negli organi collegiali (consigli di classe, interclasse/intersezione, collegio dei docenti) e comunicata formalmente a tutto il personale e attraverso materiale informativo pubblicato sul sito web;

- per proteggere tutto il personale e gli alunni, la scuola metterà in atto una linea di condotta di utilizzo accettabile, controllato e adattato alle esigenze didattiche essenziali;
- il personale docente sarà reso consapevole del fatto che il traffico in Internet può essere monitorato e si potrà risalire al singolo utente registrato;
- un'adeguata informazione/formazione del personale docente nell'uso sicuro e responsabile di Internet, sia professionalmente che personalmente, sarà fornita

a tutto il personale, anche attraverso il sito web della scuola;
- il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC sarà supervisionato dal collaboratore tecnico, che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici;
- l'Animatore Digitale evidenzierà on-line strumenti utili che il personale potrà usare con gli alunni in classe. Questi strumenti varieranno a seconda dell'età e della capacità degli alunni;
- tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

Genitori
Le linee di condotta, previste nel documento, relative ad un uso corretto della rete e delle tecnologie digitali sono state inserite nel Patto di Corresponsabilità, il quale sancisce la collaborazione scuola- famiglia nel percorso formativo degli studenti. La famiglia si rende consapevole dell'importanza di condividere la scelta di integrare l'uso delle Tic nella didattica.

- L'istituto fornirà momenti di formazione sulla sicurezza nell'uso delle tecnologie digitali e di Internet anche attraverso materiali informativi sul sitoweb della scuola
- sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di Internet in occasione degli incontri scuolafamiglia, collegiali e individuali.

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.

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) Disciplina degli alunni
Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle
tecnologie digitali e di Internet di cui si dispone per la didattica, in relazione alla fascia di età
considerata, sono prevedibilmente le seguenti:

- un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersio

partecipare;
- la condivisione online di immagini o video di compagni/e senza il loro consenso o che li ritraggono in pose offensive e denigratorie;
- la condivisione di scatti intimi;
- la condivisione di dati personali;
- il collegamento a siti web non indicati dai docenti.

Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo dell'alunno. Infatti più gli alunni sono piccoli, più i comportamenti "da correggere" sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, che devono essere compresi e orientati proprio dagli educatori nella prospettiva del raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno. Il Team delle emergenze sarà preposto all'accoglienza degli alunni incorsi in potenziali infrazioni e, a seconda della gravità dell'episodio verificatosi, potrà individuare gli interventi da adottare.
Sono previsti pertanto da parte dei docenti provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento, quali:

- il richiamo verbale;
- il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);
- il richiamo scritto con annotazione sul diario;
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente Scolastico
- coinvolgimento delle istituzioni presenti nel territorio: Forze di Polizia.

Contestualmente sono previsti interventi di carattere educativo:

- di rinforzo dei comportamenti corretti e riparativi dei disagi causati,
- di ri-definizione delle regole sociali di convivenza attraverso la partecipazione
- consapevole e attiva degli alunni della classe,
- di prevenzione e gestione positiva dei conflitti,
- di moderazione dell'eccessiva competitività,
- di promozione di rapporti amicali e di reti di solidarietà,
- di promozione della conoscenza e della gestione delle emozioni.

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.

I

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 nostro piano d'azione
La scuola promuove eventi e/o dibattiti informativi e formativi, in momenti diversidell'anno rivolti a tutto il personale, agli alunni e ai loro genitori, con il coinvolgimentodi esperti, sui temi oggetto delDocumento.
All'inizio dell'anno scolastico si prevede l'organizzazione di incontri esplicativi del progetto "GENERAZIONI CONNESSE" e del documento E-policy con la componente genitori e docenti.
Tra le misure di prevenzione che la scuola mette in atto ci sono, inoltre, azioni finalizzate a promuovere una cultura dell'inclusione, del rispetto dell'altro e delle differenze cosicché l'utilizzo di internet e dei cellulari ci collochi all'interno di unsistema di relazioni positive. A tal proposito si potrà attivare uno "Sportello di ascolto" rivolto a tutti gli alunni articolato in colloqui individuali e/o
collettivi, al fine di migliorare il benessere personale e scolastico mediante una attività di supporto della sfera emotiva, relazionale e comportamentale. Si può prevedere al suo interno uno spazio riservato ai docenti e genitori al fine di individuare strategie efficaci per affrontare problematiche tipiche dell'età adolescenziale.
Sarà previsto un Progetto curricolare nell'ambito dell'educazione civica che possa ad un tempo sviluppare le competenze digitali con la finalità di monitorare e rilevare eventuali episodi o problematiche connesse all'uso delle TIC a scuola.
I temi trattati riguarderanno la legalità intesa come :

- concetto di libero arbitrio ossia la capacità di compiere delle scelte consapevoli oppure come il risultato di un processo inconscio del cervello;
- concetto di leadership ossia lavorare con e mediante individui e/o gruppi per comprendere quali siano gli obiettivi specifici di particolari organizzazioni dedite ad attività illecite.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti, ai docenti, ai genitori

Azioni da svolgere nei prossimi 3 anni:

- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti, ai docenti, ai genitori.

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.

L'Istituto Tecnico Economico Statale "Francesco Maria Genco" prevede di ampliare il curricolo delle competenze Civiche e di Cittadinanza Digitale con le competenze Digitali, come viene descritto nell'ultima versione del DigComp 2.2:

"La competenza digitale fa parte del quadro delle competenze chiave per l'apprendimento permanente ed è interconnessa con altre competenze. La raccomandazione sulle competenze chiave per l'apprendimento permanente identifica le competenze essenziali per i cittadini per la realizzazione personale, uno stile di vita sano e sostenibile, l'occupabilità, la cittadinanza attiva e l'inclusione sociale. Tutte le competenze chiave sono complementari e interconnesse tra loro. In altre parole, le competenze essenziali per un dominio sosterranno lo sviluppo delle competenze in un altro. Questo vale anche per la competenza digitale e le altre competenze chiave."

E dalla Commissione Europea all'interno della Raccomandazione del Consiglio del 22

maggio 2018 relativa alle competenze chiave per l'apprendimento permanente.

"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."

Il curriculum verticale per lo sviluppo della competenza DIGITALE verrà strutturato sui PREREQUISITI qui di seguito descritti:

A1 A livello base, in autonomia, e risolvendo semplici problemi, sono in grado di:

• avere chiare le mie necessità di ricerca di informazioni;

• organizzare autonomamente ricerche di dati, informazioni e contenuti in ambienti digitali;

• descrivere ad altri come accedere ai dati ottenuti tramite ricerca, informazioni e contenuti e navigare al loro interno;

• organizzare informazioni, dati e contenuti affinché possano essere facilmente archiviati e recuperati in ambienti strutturati (archivi, cartelle …);

• eseguire l'analisi, il confronto, l'interpretazione, la valutazione di fonti di dati, informazioni e contenuti digitali.

A2 A livello base, in autonomia, e risolvendo semplici problemi, sono in grado di:

• conoscere e saper gestire le varie opzioni di condivisione;

• presentare/esporre in modo efficace i contenuti di una ricerca;

• utilizzare strumenti e tecnologie digitali per processi collaborativi e per co-costruzione e co-creazione di risorse e conoscenza;

• utilizzare la tecnologia per informarmi e quindi migliorare la mia capacità critica e apportare un contributo costruttivo nelle relazioni con gli altri (virtuali e non).

A3 A livello intermedio, in autonomia, e risolvendo semplici problemi, sono in grado di:

• realizzare prodotti multimediali di vario genere individualmente;

• realizzare prodotti multimediali di vario genere in modalità collaborativa;

• impartire ed interpretare istruzioni sulla base di una codifica concordata.

Ad un livello base, in autonomia, sono in grado di:

• registrarmi ad un sito online indicato dal docente;

• conoscere e rispettare le regole del diritto d'autore;

• selezionare immagini o altri materiali rispettando le regole del copyright;

• indicare le fonti di informazione;

• realizzare semplici programmi utilizzando codici di programmazione.

A4 In autonomia, e risolvendo semplici problemi, sono in grado di:

• conoscere le regole per il rispetto delle aule e dei laboratori digitali (fissi e mobili) della scuola;

• individuare e spiegare modi per proteggere i dispositivi e i contenuti digitali;

• avere cura e rispetto dei miei strumenti digitali e di quelli altrui;

• distinguere l'ambiente virtuale da quello reale;

• conoscere i vantaggi e i rischi degli ambienti digitali;

• scegliere semplici modi per proteggere i miei dati personali e la mia privacy (ad es. conoscere i rischi legati alla pubblicazione di immagini personali);

• riconoscere i rischi legati alla salute psicologica e fisica quando utilizzo le tecnologie digitali;

• adottare semplici atteggiamenti sostenibili (non dimenticare i dispositivi accesi, usare le funzioni di risparmio energetico, ecc.);

• essere consapevoli dell'importanza di utilizzare la terminologia adeguata per comunicare sui canali social.

A5 A livello intermedio, in autonomia, sono in grado di:

• individuare e risolvere i più comuni e semplici problemi tecnici relativi ai dispositivi

(computer fisso, tablet, monitor/LIM, ecc.) e agli ambienti digitali;

• usare con dimestichezza strumenti e tecnologie digitali per elaborare soluzioni adatte a migliorare il mio apprendimento;

• adattare e personalizzare gli ambienti digitali secondo le mie esigenze (ad es. per l'accessibilità o la facilità d'uso);

• essere consapevole della necessità di sviluppare e potenziare la mia competenza digitale;

• conoscere le nuove opportunità offerte dalle tecnologie digitali in continua evoluzione.

La progettazione terrà presente le 5 AREE e le 21 COMPETENZE

Area di competenza 1. Alfabetizzazione su informazioni e dati

Descrittori di competenza:
1.1 Navigare, ricercare e filtrare le informazioni e i contenuti digitali
1.2 Valutare dati, informazioni e contenuti digitali
1.3 Gestire dati, informazioni e contenuti digitali

Area di competenza 2. Comunicazione e collaborazione
Descrittori di competenza:
2.1 Interagire con gli altri attraverso le tecnologie digitali
2.2 Condividere informazioni attraverso le tecnologie digitali
2.3 Esercitare la cittadinanza attraverso le tecnologie digitali
2.4 Collaborare attraverso le tecnologie digitali
2.5 Netiquette
2.6 Gestire l'identità digitale

Area di competenza 3. Costruzione di contenuti
Descrittori di competenza:
3.1 Sviluppare contenuti digitali
3.2 Integrare e rielaborare contenuti digitali
3.3 Copyright e licenze
3.4 Programmazione

Area di competenza 4. Sicurezza
Descrittori di competenza:
4.1 Proteggere i dispositivi
4.2 Proteggere i dati personali e la privacy
4.3 Proteggere la salute e il benessere
4.4 Proteggere l'ambiente

Area di competenza 5. Risolvere problemi
Descrittori di competenza:
5.1 Risolvere problemi tecnici
5.2 Individuare bisogni e risposte tecnologiche
5.3 Utilizzare in modo creativo le tecnologie digitali
5.4 Individuare i divari di competenze digitali

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.

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

2.3 - Formazione dei docenti sull'utilizzo consapevole e sicuro di

Internet e delle tecnologie digitali

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

Coerentemente con quanto previsto dal PNSD, l'Istituto si avvale dell'Animatore Digitale, che coordina la diffusione dell'innovazione digitale e collabora con tutti i soggetti che possono contribuire alla realizzazione degli obiettivi del Piano.

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 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.

Inoltre, a partire dall'anno scolastico 2022/2023 è attiva la figura del Referente d'Istituto per le attività di prevenzione e contrasto al bullismo e cyberbullismo (L.107/2015). La formazione sull'utilizzo consapevole e sicuro delle TIC è stata estesa ad altre figure, in funzione della costituzione di un Team per le Emergenze. Si rende, comunque, necessaria la formazione di tutti i docenti sull'uso consapevole e sicuro di Internet e sui rischi della rete.

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.

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

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023)

- 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)

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'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.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

In merito alla protezione dei dati personali, si fa riferimento a quanto previsto dal Regolamento Europeo 2016/679, nel seguito indicato sinteticamente come Regolamento e del Decreto Legislativo 30 giugno 2003, n. 196 ("Codice in materia di protezione dei dati personali") nel seguito indicato sinteticamente come Codice, il trattamento dei dati personali sarà improntato ai principi di correttezza, liceità, trasparenza e tutela della riservatezza dei diritti degli alunni e delle rispettive famiglie. Pertanto, ai sensi dell'art. 13 del Regolamento, forniamo le seguenti informazioni:

Oggetto del trattamento

Il Titolare del trattamento tratta i dati personali, identificativi (ad esempio, nome, cognome, indirizzo, telefono, e-mail, riferimenti bancari e di pagamento) o di natura particolare (dati sanitari o giudiziari) da Lei comunicati. Il conferimento dei dati richiesti è obbligatorio in quanto necessario alla realizzazione delle finalità istituzionali. L'eventuale diniego al trattamento di tali dati potrebbe comportare il mancato perfezionamento dell'iscrizione e l'impossibilità di fornire all'alunno tutti i servizi necessari per garantire il suo diritto all'istruzione ed alla formazione.

Dati obbligatori. I dati personali obbligatori da fornire, strettamente necessari all'esercizio delle funzioni istituzionali, sono i seguenti. Per quanto riguarda l'allievo: nome e cognome dell'alunno, data e luogo di nascita, indirizzo e numero telefonico, titolo di studio, attestati di esito scolastico e altri documenti e dati relativi alla carriera scolastica, foto ed eventuale certificato d'identità, certificati medici o altre dichiarazioni per la riammissione a scuola in caso di assenza, e in determinati casi certificazione di vaccinazione; Per quanto riguarda la famiglia dell'allievo: nome e cognome dei genitori o di chi esercita la potestà genitoriale, data e luogo di nascita, indirizzo e numero telefonico, se diversi da quelli dell'alunno. I dati personali qualificati dal Regolamento UE 2016/679 come particolari categorie di dati e dunque di natura sensibile e giudiziaria verranno trattati nel rispetto del principio di indispensabilità del trattamento. Di norma non saranno soggetti a diffusione, salvo la necessità di comunicare gli stessi ad altri Enti Pubblici nell'esecuzione di attività istituzionali previste da norme di legge in ambito sanitario (quali ad esempio gli adempimenti connessi all'emergenza sanitaria COVID-19), previdenziale, tributario, infortunistico, giudiziario, collocamento lavorativo. L'acquisizione e il trattamento di questa duplice tipologia di dati avverranno secondo quanto previsto da disposizioni di legge ed in considerazione delle finalità di rilevante interesse pubblico che la scuola persegue.

Dati facoltativi. Per taluni procedimenti amministrativi attivabili soltanto su domanda

individuale (ottenimento di particolari servizi, prestazione, benefici, esenzioni, certificazioni, ecc.) può essere indispensabile il conferimento di ulteriori dati, altrimenti la finalità richiesta non sarebbe raggiungibile. In tali casi verrà fornita un'integrazione verbale della presente informativa.

Finalità del trattamento e base di legge

I dati personali forniti saranno trattati unicamente per le finalità istituzionali della scuola, che sono quelle relative all'istruzione ed alla formazione degli alunni e quelle amministrative ad esse strumentali, così come sono definite dalla normativa statale e regionale. I dati personali sono trattati senza il consenso espresso ai sensi dell'art. 6 lett. b), c) ed e) del GDPR, per le seguenti finalità:

- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; - il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. I dati personali di carattere particolare sono trattati ai sensi dell'art. 9, comma 2, lett. g) del GDPR e dunque g) "il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato". Ai sensi dell'art. 2 sexies D.Lgs. 196/03, come modificato dal D.Lgs. 101/2018, si considera di rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri, ai sensi della lett. bb), "l'attività di istruzione e formazione in ambito scolastico, professionale, superiore o universitario" In ogni caso il trattamento avverrà sempre nel rispetto dei diritti e delle libertà dell'interessato assicurando:

a) che lo stesso sia proporzionato alla finalità perseguita;

b) che sia salvaguardata l'essenza del diritto alla protezione dei dati;

c) che siano previste misure appropriate e specifiche per tutelare i diritti e le libertà fondamentali dell'interessato nonché nel rispetto delle misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute disposte dall'Autorità Garante per la Protezione dei Dati Personali prevedendo che il consenso, ove richiesto, venga manifestato liberamente.

Modalità di acquisizione e di trattamento dati

I dati personali dell'alunno e dei familiari vengono acquisiti direttamente dall'alunno stesso, dai genitori o dalla scuola di provenienza nel caso dei trasferimenti o da altre pubbliche amministrazioni. A garanzia dei diritti dell'Interessato, il trattamento dei

dati è svolto secondo le modalità e le cautele previste dalla normativa vigente. Il trattamento può essere svolto in forma cartacea, o attraverso strumenti informatici e telematici, ed i relativi dati saranno conservati, oltre che negli archivi presenti presso la presente istituzione scolastica, anche presso gli archivi del Ministero dell'Istruzione e suoi organi periferici (Ufficio Scolastico Regionale, Ambito Territoriale Provinciale, ed altri). In tal caso i dati verranno trattati e conservati secondo le regole tecniche di conservazione digitale indicate dall'AGID. I dati cartacei, invece, secondo quanto previsto dai piani di conservazione e scarto indicati dalla direzione generale degli archivi presso il Ministero dei beni culturali. Il trattamento prevede come fasi principali: raccolta, registrazione, organizzazione, conservazione, elaborazione, comunicazione, diffusione e cancellazione dei dati quando questi cessino di essere necessari.

Comunicazione e diffusione dei dati

I soggetti a cui i dati personali potranno essere comunicati nell'ambito della scuola sono: il Dirigente Scolastico, i Responsabili o Designati del trattamento (D.S.G.A. e Collaboratore Vicario), gli Autorizzati del trattamento amministrativo (che di fatto corrispondono alla segreteria amministrativa), i docenti del Consiglio di classe ed i membri dell'equipe per l'integrazione scolastica, relativamente ai dati necessari alle attività didattiche, di valutazione, integrative e istituzionali. Inoltre, i dati possono essere comunicati anche ai collaboratori scolastici ed i componenti degli organi collegiali limitatamente a quelli strettamente necessari alla loro attività. I dati personali, diversi da quelli sensibili e giudiziari, potranno essere comunicati ad altri enti pubblici o privati esclusivamente nei casi previsti da leggi e regolamenti (in particolare: altre strutture del sistema della Pubblica Istruzione, altre strutture pubbliche, INAIL, Azienda Sanitaria pubblica competente, Società di Assicurazione per polizza infortuni, Agenzie viaggi, Software house). I dati da Lei forniti potranno essere comunicati a terzi soggetti che forniscono servizi a codesta Istituzione scolastica quali, a titolo esemplificativo, agenzie di viaggio e strutture ricettive (esclusivamente in relazione a gite scolastiche, viaggi d'istruzione e campi scuola), imprese di assicurazione (in relazione a polizze in materia infortunistica), eventuali ditte fornitrici di altri servizi (quali ad esempio servizi di mensa, software gestionali, registro elettronico, servizi digitali, piattaforme di Didatti Digitale, ecc…). La realizzazione di questi trattamenti costituisce una condizione necessaria affinché l'interessato possa usufruire dei relativi servizi; in caso di trattamenti continuativi, le ditte in questione sono nominate responsabili del trattamento, limitatamente ai servizi resi. Potranno essere diffusi esclusivamente i dati previsti dalla normativa e rigorosamente nei casi ivi indicati. I dati relativi agli esiti scolastici degli alunni potranno essere pubblicati mediante affissione all'albo della scuola o all'albo online nei limiti delle vigenti disposizioni in materia. L'Istituzione scolastica tratta i dati contenuti nei documenti di valutazione e orientamento degli alunni per l'assolvimento delle finalità di documentazione dei processi formativi e di orientamento degli alunni. Per tali ragioni, il loro conferimento è obbligatorio, in quanto necessario per perseguire le suddette finalità istituzionali. Si fa inoltre presente che è possibile che foto di lavori e di attività

didattiche afferenti ad attività istituzionali della scuola inserite nel Piano dell'Offerta Formativa (quali ad esempio foto relative ad attività di laboratorio, visite guidate, premiazioni, partecipazioni a gare sportive, ecc.) vengano utilizzate per fini istituzionali e di documentazione e quindi pubblicate sul sito istituzionale e/o sul giornalino scolastico o altre testate giornalistiche locali e nazionali, su poster o manifesti dell'istituto, anche in occasione di partecipazione a fiere e attività di promozione relative all'orientamento scolastico; è inoltre possibile vengano effettuate durante l'anno foto di classe o riprese, da parte della scuola, di alcune attività didattiche e istituzionali. In caso di pubblicazione di immagini e/o video sul sito istituzionale o pagine social della scuola il trattamento avrà natura temporanea dal momento che le suddette immagini e video resteranno sul sito solo per il tempo necessario per la finalità cui sono destinati. Nei video e nelle immagini di cui sopra i minori saranno ritratti solo nei momenti "positivi" legati alla vita della scuola: apprendimento, recite scolastiche, competizioni sportive, ecc. Si fa presente che per ulteriori informazioni e delucidazioni, o per segnalare la volontà di non aderire a determinate iniziative o servizi tra quelli indicati è possibile rivolgersi al titolare o designato del trattamento dei dati personali della scuola, indicato di seguito. Gli studenti e gli altri membri della comunità scolastica, in ogni caso, non possono diffondere o comunicare sistematicamente i dati di altre persone (ad esempio pubblicandoli su Internet) senza averle prima informate adeguatamente e averne ottenuto l'esplicito consenso.

Titolare, responsabile e incaricati

Il Titolare del trattamento è l'ISTITUTO TECNICO ECONOMICO STATALE "Francesco Maria Genco", in persona del suo legale rappresentante Dirigente Scolastico prof. Leonardo CAMPANALE con sede legale in piazza Laudati n. 1 ad Altamura (BA).

Il Responsabile della Protezione dei Dati (RPD) è l'Avv. Nicola Parisi con studio in Noicàttaro (BA) alla Via Carducci 46 raggiungibile a mezzo mail all'indirizzo: parisi@actioavvocati.it a mezzo PEC all'indirizzo: nicolaparisi@legalmail.it e al numero di telefono 0804782868.

Diritti dell'interessato

L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile. Ove applicabili, all'interessato sono riconosciuti i diritti di cui agli artt. 16-21 GDPR (Diritto di rettifica, diritto all'oblio, diritto di limitazione di trattamento, diritto alla portabilità dei dati, diritto di opposizione) nonché il diritto di reclamo all'Autorità Garante.

Modalità di esercizio dei diritti

Potrà in qualsiasi momento esercitare i diritti inviando richiesta al Titolare tramite: - e-mail all'indirizzo batd02000a@istruzione.it - PEC all'indirizzo batd02000a@pec.istruzione.it - posta all'indirizzo: piazza Laudati n. 1 Altamura (BA)

cap 70022

Ha altresì il diritto di reclamo diretto all'Autorità Garante che può essere esercitato tramite apposita procedura sul sito del Garante www.garanteprivacy.it.

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.

Premesso che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi ai principi della diligenza e correttezza, normalmente rispettati nell'ambito dei rapporti di lavoro, L'Istituto Scolastico adotta un Regolamento interno finalizzato ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti i soggetti autorizzati, in attuazione del REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Considerato che, inoltre, l'Istituto Scolastico, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, mette a disposizione dei propri dipendenti, a seconda del tipo di funzioni svolte, mezzi di comunicazione efficienti (computer etc.), sono state inserite nel regolamento alcune clausole relative alle modalità ed i doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

La finalità è quella di verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet, muovendo dalla considerazione che prevenire gli abusi debba considerarsi più importante che individuarli.

I principi costituenti il fondamento del presente Regolamento sono gli stessi espressi nel REGOLAMENTO (UE) 2016/679 e nel documento "Lavoro: le linee guida del Garante per posta elettronica e internet" del 01/03/2007, e, precisamente:

a) il principio di necessità, per il quale l'utilizzo dei dati personali, attraverso l'impiego di sistemi informativi e di programmi informatici, deve essere ridotto al minimo tenuto conto delle finalità perseguite;

b) il principio di correttezza, per il quale le caratteristiche essenziali dei trattamenti, siano essi svolti in modalità cartacea o informatica oppure mista (cartacea ed informatica), devono essere partecipate ai lavoratori;

c) le finalità alla base del trattamento dei dati personali devono essere determinate, esplicite e legittime, oltre che pertinenti e non eccedenti.

Alla luce dell'art. 4, comma 1, L. 300/1970, la regolamentazione della materia indicata nell'art. 1 del presente Regolamento, non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo per consentire a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.

Regolamento

4. Gestione ed assegnazione delle credenziali di autenticazione

4.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal Titolare del Trattamento. 4.2 Le credenziali di autenticazione consistono in un codice

per l’identificazione dell’utente (user id), associato ad una parola chiave (password) riservata che dovrà essere custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione, senza preventiva autorizzazione da parte del Titolare del Trattamento.

4.3 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri e/o simboli, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all’incaricato.

4.4 È necessario procedere alla modifica della parola chiave, a cura dell’utente incaricato del trattamento, al primo utilizzo e successivamente ogni volta in cui vi è una indicazione in tal senso o si ritiene che la password possa essere stata conosciuta da terzi e/o colleghi.

4.5 Qualora fosse necessaria la sostituzione della parola chiave in seguito alla perdita della propria riservatezza, si procederà in tal senso.

4.6 Soggetto preposto alla custodia delle credenziali di autenticazione è Titolare del Trattamento.

5. Utilizzo della rete dell’Istituto Scolastico

5.1 Per l’accesso alla rete ciascun utente deve essere in possesso delle specifiche credenziali di autenticazione.

5.2 È assolutamente proibito entrare nella rete e nei programmi con un codice d’identificazione utente diverso da quello assegnato. Le parole chiave d'accesso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

5.3 Le cartelle utenti presenti nei server sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file non inerente all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup da parte del Titolare del Trattamento.

5.4 Il Titolare del Trattamento può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà pericolosi per la Sicurezza sulle unità di rete.

5.5 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

8. Uso della posta elettronica

8.1 La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le

persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

8.2 È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per: - l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa; - l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list; - la partecipazione a catene telematiche (o "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo si deve comunicare immediatamente al Titolare del Trattamento. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

8.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

9. Navigazione in Internet

9.1 Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

9.2 In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:

- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione;

- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati nel rispetto delle normali procedure di acquisto;

- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;

- la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio;

- l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

9.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Istituzione scolastica rende nota, peraltro, l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o

l’accesso a determinati siti inseriti in una black list.

9.4 Gli eventuali controlli, compiuti dal Titolare del Trattamento ai sensi del precedente punto 3.3, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante “file di log”. In applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all’accesso ad Internet ed al traffico telematico (log di sistema e del server proxy), la cui conservazione non sia necessaria, saranno cancellati entro tre mesi dalla loro produzione, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell’amministrazione. In casi eccezionali (es.: esigenze tecniche o di sicurezza; indispensabilità dei dati rispetto all’esercizio o alla difesa di un diritto in sede giudiziaria; obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell’autorità giudiziaria o della polizia giudiziaria) è consentito il prolungamento dei tempi di conservazione limitatamente al soddisfacimento delle esigenze sopra esplicitate.

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.

A tale proposito è importante effettuare una distinzione preliminare fra comunicazione interna e comunicazione esterna. Diversi strumenti di comunicazione online possono essere utilizzati dalla scuola, sia per raggiungere target esterni, al fine di valorizzare e promuovere le attività portate avanti dall’Istituto (rivolgendosi ad esempio a istituzioni, famiglie, studenti non ancora iscritti, associazioni etc.) sia per far circolare all’interno della scuola informazioni di servizio o contenuti importanti fra i diversi attori scolastici (docenti, studenti, genitori, collaboratori scolastici etc.). Fra gli strumenti di comunicazione esterna, ad esempio, troviamo il sito web della scuola, i social network con le pagine Facebook e Istagram.

Il sito dell ' ITES è raggiungibile all ’ indirizzo www.itesgenco.edu.it

La gestione del sito della scuola e la rispondenza allenormative per quanto concerne i contenuti (accuratezza, appropriatezza, aggiornamento) e le tecniche di realizzazione e progettazione è a cura del Dirigente Scolastico e dell’Animatore Digitale. Sul sito è

possibile trovare il Regolamento d'Istituto, pubblicizzazione di eventi, avvisi ai genitori, documentazione di attività curricolari ed extracurricolari svolte; pulsanti attivi permettono l'accesso a link di interesse, tra cui il registro elettronico.

La scuola, in qualità di ente pubblico, pubblicherà sul proprio sito web i contenuti che saranno valutati come pertinenti alle finalità educative istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative.

Fra gli strumenti di comunicazione interna troviamo:

- il RE (Registro Elettronico)strumento essenziale a disposizione delle scuole per la gestione di assenze, presenze, valutazioni, prenotazioni di incontri e comunicazioni con le famiglie al fine di permettere un costante monitoraggio da parte delle famiglie e della scuola sull'andamento dell'alunno
- l'e-mail destinata alla ricezione di comunicazioni, all'invio di documentazione, alla condivisione di materiali, progetti e materiali con altri docenti.
- piattaforme di lavoro condiviso e collaborativo come G-Suite e Webex.

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 Ministro dell'Istruzione e del Merito, con Nota N. 107190 del 19/12/2022 "Indicazioni sull'utilizzo dei telefoni cellulari e analoghi dispositivi elettronici in classe", ha richiamato all'obbligo da parte degli alunni di divieto dell'suo del cellulare

durante le ore di lezione. In particolare si richiama l'attenzione su quanto previsto anche nello Statuto delle studentesse e degli studenti, di cui al D.P.R. 24 giugno 1998, n. 249": "l'uso del cellulare e di altri dispositivi elettronici rappresenta un elemento di distrazione sia per chi lo usa che per i compagni, oltre che una grave mancanza di rispetto per il docente configurando, pertanto, un'infrazione disciplinare sanzionabile attraverso provvedimenti orientati non solo a prevenire e scoraggiare tali comportamenti ma anche, secondo una logica educativa propria dell'istituzione scolastica, a stimolare nello studente la consapevolezza del disvalore dei medesimi". L'uso dei dispositivi digitali, tuttavia, è consentito quali strumenti compensativi con il consenso del docente, per finalità inclusive, didattiche e formative, anche nel quadro del Piano Nazionale Scuola Digitale e degli obiettivi della c.d. "cittadinanza digitale" di cui all'art. 5 L. 25 agosto 2019, n. 92. Si precisa, infine, che il Regolamento disciplinare del nostro istituto, prevede già specifiche sanzioni disciplinari per l'uso improprio del telefonino (art. 18 del regolamento di Istituto): http://itesgenco.edu.it/index.php/offerta-formativa/regolamenti Per quanto attiene il Personale scolastico, l'uso del cellulare è consentito per motivi di servizio o di accesso alle risorse digitali della scuola (registro elettronico, ..). Si invitano, infine, le famiglie a collaborare e a vigilare affinché i propri figli rispettino tali disposizioni finalizzate esclusivamente a rendere più efficace e produttivo lo svolgimento delle attività didattiche. Gli alunni, possono portare con sé il cellulare, poiché utile a contattare le famiglie dopo l'uscita da scuola, ma sono tenuti a spegnerlo al momento dell'ingresso.

E' fatto assoluto divieto da parte degli alunni di contattare la famiglia con il proprio cellulare per richiedere materiale scolastico dimenticato o per richiedere di essere prelevati prima del termine delle lezioni. I genitori che dovessero presentarsi a scuola perché contattati direttamente dai propri figli con il proprio cellulare e senza autorizzazione del docente, saranno ritenuti corresponsabili della eventuale sanzione disciplinare.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023).

- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

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

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

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

L'ITES “Francesco Maria Genco” intende perseguire azioni di prevenzione universale e di sensibilizzazione, attraverso un'efficace integrazione con la rete dei servizi territoriali locali (Polizia Postale, ASL, USR...), al fine di formare e consolidare quelle competenze educative di base necessarie per poter gestire le situazioni di vita che i ragazzi sperimentano online. Nello specifico, la scuola , attiverà una serie di misure:

- integrare nel curricolo temi legati al corretto utilizzo delle TIC e di Internet;
- progettare unità didattiche specifiche che verranno pianificate a livello delle aree disciplinari, garantendo un intervento su ogni classe;
- supportare e implementare la competenza digitale in tutti i ragazzi all’interno delle materie curricolari.

Si demanda alle aree disciplinari la scelta dei settori su cui focalizzare la formazione.

4.2 - Cyberbullismo: che cos’è e come prevenirlo

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

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

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

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;

- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
  - Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
  - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Il cyberbullismo presenta le seguenti caratteristiche:

- è invasivo: il bullo può raggiungere la sua vittima in qualsiasi momento e in qualunque luogo;
- è un fenomeno persistente: il materiale messo online vi può rimanere per molto tempo;
- ha una platea potenzialmente infinita: le persone che possono assistere agli atti di cyberbullismo sono potenzialmente illimitate.

A seconda dei casi, si potranno adottare azioni di prevenzione universale, selettiva e indicata

Prevenzione Universale: tutti gli studenti sono potenzialmente a rischio. Si attivano interventi diretti al grande pubblico o ad un intero gruppo di una popolazione che non è stato identificato sulla base del rischio individuale.

Efficacia: un programmi ad ampio raggio può avere effetti modesti se confrontato con programmi che "trattano" problematiche specifiche di un gruppo. Tuttavia, questi interventi possono produrre cambiamenti in grandi popolazioni (ad es. si pensi ad un programma dedicato alle competenze emotive, oppure alla cittadinanza digitale).

Prevenzione Selettiva: un gruppo di studenti in cui il rischio online è presente. In questo caso la presenza del rischio è stata individuata tramite precedenti indagini, segnalazioni fatte dalla scuola, oppure dalla conoscenza della presenza di fattori di rischio in quel determinato territorio.

Efficacia: gli interventi sono mirati e prevedono programmi formativi strutturati che hanno l'obiettivo di migliorare le competenze digitali e le strategie di problem solving. Può essere un valido programma se si osservano casi in cui la prevenzione universale non ha dato gli esiti previsti.

Prevenzione Indicata: un caso specifico è pensato e strutturato per adattarsi agli/lle studenti/studentesse con l'obiettivo di ridurre i comportamenti problematici, oppure dare supporto alle vittime. Per la sua natura questo tipo di intervento si avvale di professionalità diverse perché spesso affronta problemi legati alla salute mentale del

minore per cui è opportuno coinvolgere anche la famiglia del/lla ragazzo/a.

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.

Inoltre, l'Istituto si potrà avvalere di consulenti/esperti esterni (Carabinieri, PoliziaPostale, equipe Formazione Territoriale del MIUR, associazioni del Territorio) per organizzare incontri formativi rivolti a docenti, genitori ed alunni con lo scopo di rendere consapevoli gli attori del fenomeno descritto.

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?

Gli elementi che contribuiscono al benessere digitale sono:

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

È importante non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli studenti e delle studentesse, strutturando chiare e semplici regole condivise, ossia stipulare con gli studenti una sorta di "patto" d'aula e proporre delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d'aula.

Inoltre, sarà fondamentale concordare una linea condivisa con la famiglia, per stabilire mezzi e modalità durante lo studio domestico, con forme di controllo attivo durante la navigazione in Rete.

4.5 - Sexting

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

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

I contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di "revenge porn", letteralmente "vendetta porno", fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/i e depressione.

Se si rilevano casi di lieve entità occorre in primo luogo parlarne con alunne e alunni e rispettivi genitori, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. Chi è immerso dalla nascita nelle nuove tecnologie spesso non è consapevole che una foto o un video diffusi in rete potrebbero non essere tolti mai più né è consapevole di scambiare o diffondere materiale pedopornografico.

In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico per gli adempimenti del caso.

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.

La problematica dell'adescamento online (come quella del sexting) si inquadra in uno scenario più ampio di scarsa educazione emotiva, sessuale e di assenza di competenza digitale.

Al fine di prevenire casi di adescamento online è opportuno, pertanto, accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla

sessualità. Ciò aiuterebbe a renderli emotivamente più sicuri e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri.

È importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato.

Fondamentale quindi, è portare avanti un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è).

Se si sospetta o si ha la certezza di un caso di adescamento online è importante che l'adulto di riferimento non si sostituisca al minore nel rispondere, ad esempio, all'adescatore. È importante che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove. Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot,

memorizzando eventuali immagini o video…). L'adescamento, inoltre, può essere unaproblematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.

Nei casi più estremi in cui si accerta che l'adescamento porta ad un incontro fisico e ad un abuso sessuale un sostegno psicologico esperto per il minore è da considerarsi prioritario e urgente.

4.7 - Pedopornografia

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

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

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

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

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

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

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

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

ancora in corso e il supporto necessario.

Parallelamente, per salvaguardare il benessere psicofisico degli alunni coinvolti nella visione di questi contenuti, sarà opportuno ricorrere a un supporto psicologico anche passando per una consultazione presso il medico di base o pediatra di riferimento. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza: Consultori Familiari, Servizi di Neuropsichiatria infantile, centri specializzati sull'abuso e il maltrattamento all'infanzia, etc.

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

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

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

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

Polizia di Stato "Commissariato online".

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

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023).

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

□ Organizzare uno o più incontri 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.

□ 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.

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

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

□ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.

□ 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.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e

studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per

segnalare la presenza di materiale pedopornografico online.

Pertanto sono da considerare degni di segnalazione:

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

Le/gli insegnanti in particolare sono chiamati a essere spazio di avamposto privilegiato delle problematiche, dei rischi, dei pericoli che gli adolescenti possono vivere e affrontare ogni giorno. Accorgersi tempestivamente di quanto accade e compiere azioni immediate di contrasto verso gli atti inopportuni -quando non illegali- diviene fondamentale per poter evitare conseguenze a lungo termine che possano pregiudicare il benessere e una crescita armonica dei soggetti coinvolti.

5.2. - Come segnalare: quali strumenti e a chi

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

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

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

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

bullismo e/o cyberbullismo, sexting o adescamento online.

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

Strumenti a disposizione di studenti/esse

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

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

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

Per quanto riguarda la gestione dei casi, il nostro Istituto ha individuato una figura referente per il cyberbullismo. La segnalazione del caso dovrà quindi essere fatta dal singolo docente, tramite modulo allegato al presente documento (Allegato 2), alla referente, la quale, insieme al Team per le emergenze, si occuperà di raccogliere tutte le informazioni possibili, anche attraverso colloqui di approfondimento con gli attori coinvolti e di segnalare l'accaduto al Dirigente. Sarà poi il Dirigente, insieme al Team, a valutare se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali o se il caso vada gestito all'interno della scuola con il coinvolgimento del Consiglio di Classe e delle famiglie degli alunni coinvolti. Si sceglierà uno o più interventi da attuare a cui seguirà una fase di monitoraggio. (cfr. schema di procedura di intervento (nell'Allegato 3)

5.3. - Gli attori sul territorio

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

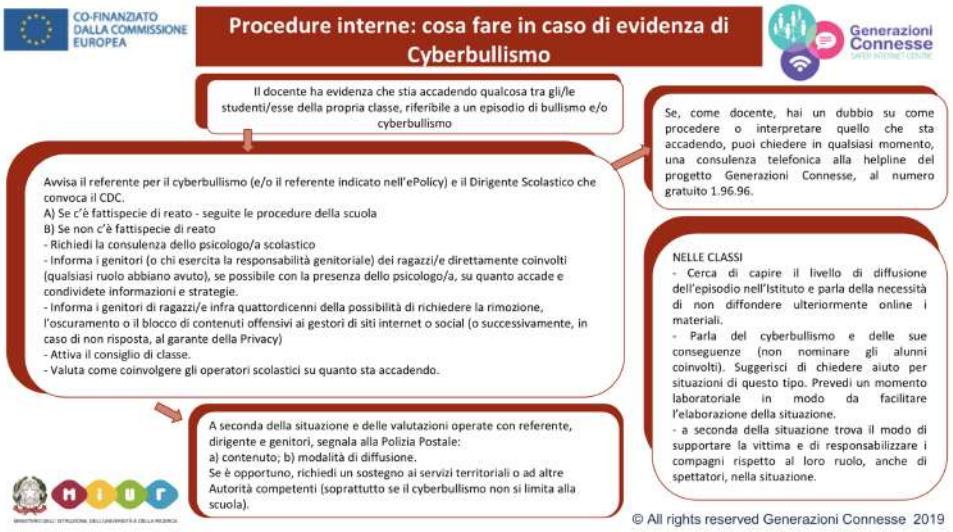
Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza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

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

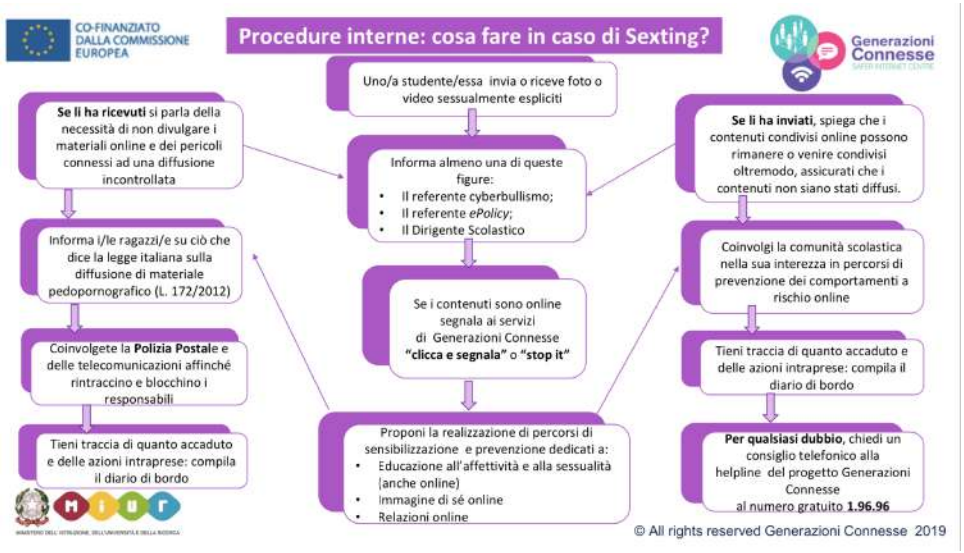
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

5.4. - Allegati con le procedure

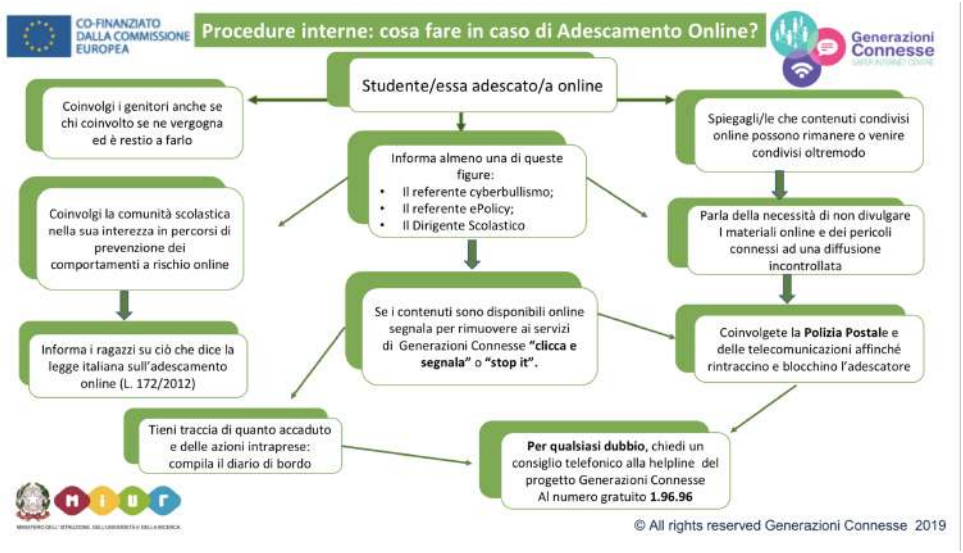
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



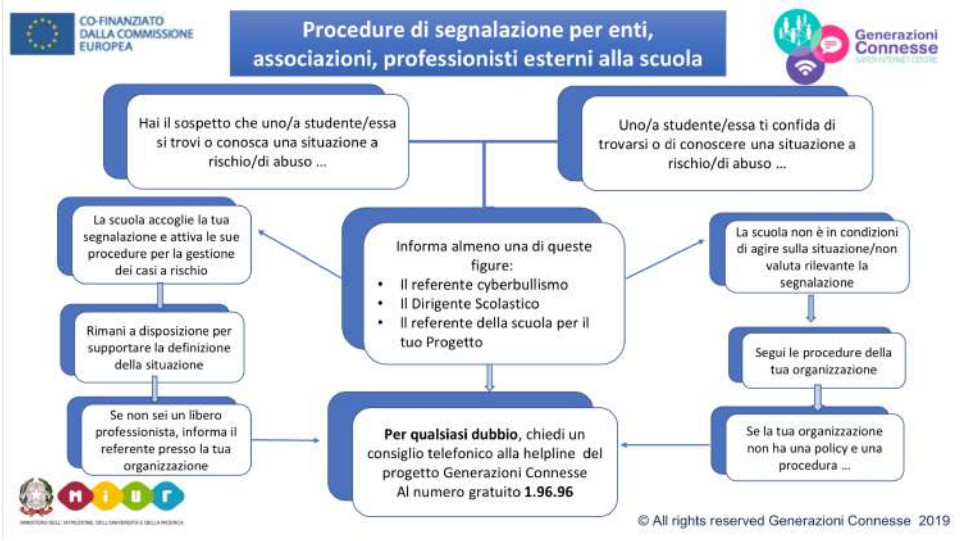
Procedure interne: cosa fare in caso di sexting?



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

ALLEGATO 2

Modulo di prima segnalazione dei casi di (presunto) bullismo e vittimizzazione

Nome di chi compila la segnalazione: Nome Cognome_____
nato a_____
il __/__/___ Data:_____ Scuola: _____

1. **La persona che ha segnalato il caso di presunto bullismo era: (selezionare tra le voci che seguono)**
   - o La vittima: Nome _____Cognome_____ nato a_____ il __/__/___
   - Un compagno vittima: Nome Cognome_____ nato a_____ il __/__/
   - Madre/Padre/ Tutore vittima: Nome Cognome nato

a_____ il __ /___ / ___
- Insegnante: Nome _____Cognome _____nato a_____ il __ /___ / ___
- Altri_____ : Nome Cognome_____ nato a_____ il __ /___ / ___

2. Vittima:_____ Classe: _____

Altre vittime:_____ Classe: _____

Altre vittime: _____ Classe: _____

3. Bullo/i (o presunti)

Nome:_____ Classe: _____

Nome:_____ Classe:_____

Nome: _____ Classe: _____

4. Descrizione breve del problema presentato. Dare esempi concreti degli episodi di prepotenza.

_____
____
_____
____
_____
____

5. Quante volte sono successi gli episodi?

_____
___
_____
____

Altamura,____/____/____

Firma del segnalatore

ALLEGATO 3

Valutazione approfondita dei casi di bullismo e vittimizzazione

1. Data della segnalazione del caso di bullismo:

2. La persona che ha segnalato il caso di bullismo era:

• La vittima:

• Un compagno della vittima, nome:

• Madre/ Padre della vittima, nome

• Insegnante, nome

• Altri:

3. Nome e ruolo della persona della scuola che ha compilato il modulo del pre-screening:

4. Vittima, nome: _____Classe: _____

Altre vittime, nome:_____ Classe: _____

Altre vittime, nome_____ Classe: _____

5. Il bullo o i bulli

Nome:_____ Classe: _____

Nome:_____ Classe: _____

Nome:_____ Classe: _____

6. Che tipo di prepotenze sono accadute? Dare esempi concreti degli episodi:

7. In base alle informazioni raccolte, che tipo di bullismo è avvenuto?

Osservazioni (indicare Si o No)	**Si /No**
è stato offeso, ridicolizzato e preso in giro in modo offensivo;	
è stato ignorato completamente o escluso dal suo gruppo di amici;	
è stato picchiato, ha ricevuto dei calci, o è stato spintonato;	
sono stati messe in giro bugie/voci che hanno portato gli altri ad "odiarlo";	
gli sono stati presi dei soldi o altri effetti personali (o sono stati rotti);	
è stato minacciato o obbligato a fare certe cose che non voleva fare;	
gli hanno dato dei brutti nomi, hanno fatto brutti commenti o gesti sulla sua etnia, colore della pelle, religione, orientamento sessuale o identità di genere;	
ha subito delle offese o molestie sessuali, attraverso brutti nomi, gesti o atti;	
è stato escluso da chat di gruppo, da gruppi WhatsApp, o da gruppi online;	
ha subito le prepotenze online tramite computer o smartphone con messaggi offensivi, post o fotografie su Facebook, su WhatsApp, Twitter, Myspace, Snapchat o tramite altri social media	
ha subito appropriazione di informazioni personali e utilizzo sotto falsa identità della propria password, account (e-mail, Facebook…), rubrica del cellulare…	

Altro:

8. Quante volte sono successi gli episodi di bullismo?

9. Quando è successo l'ultimo episodio di bullismo?

10. Da quanto tempo il bullismo va avanti?

11. Si sono verificati episodi anche negli anni precedenti?

12 Sofferenza della vittima: (indicare con una X sotto alla colonna scelta)

La vittima presenta…	**Non vero**	**In parte - Qualche volta vero**	**Molto vero Spesso Vero**
Cambiamenti rispetto a come era prima			
Ferite o dolori fisici non spiegabili			
Paura di andare a scuola (non va volentieri)			

Paura di prendere l'autobus –
richiesta di essere accompagnato-
richiesta di fare una strada diversa
Difficoltà relazionali con i compagni
Isolamento / rifiuto
Bassa autostima
Cambiamento nell'umore generale (è più triste, depressa, sola/ritirata)
Manifestazioni di disagio fisico-comportamentale (mal di testa, mal di pancia, non mangia, non dorme…)
Cambiamenti notati dalla famiglia
Impotenza e difficoltà a reagire

Gravità della situazione della vittima (indicare con una X sotto alla colonna scelta):

Il nostro piano d'azioni

Non è prevista nessuna azione.