Documento di ePolicy

PAIC8AG007

I.C. CARINI-CALDERONE/TORRETTA

VIA EMILIA1 - 90044 - CARINI - PALERMO (PA)

CLAUDIA NOTARO

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.

Gli alunni sono sempre più esposti in maniera precoce a occasioni di interazione con Internet attraverso una gamma sempre più ricca di dispositivi facilmente alla loro portata. L'accesso in rete, soprattutto per i bambini e gli adolescenti, se da una parte, rappresenta un'opportunità di accrescimento del sapere, di incremento delle capacità comunicative, di sviluppo delle competenze e di miglioramento delle prospettive di lavoro, dall'altra, tuttavia, può esporre gli stessi a situazioni di vulnerabilità che richiedono interventi specifici. In questi ultimi anni, è diventato sempre più forte il bisogno di adottare una strategia che si faccia carico di fornire risposte adeguate a "nuovi" bisogni. Questo implica lo sviluppo di servizi rivolti ai/alle ragazzi/e dal contenuto innovativo e di più alta qualità, che garantiscano loro di muoversi in sicurezza e con competenza negli ambienti digitali.

Il ruolo del MIUR nel creare un "*Better Internet for Kids*"

Il Ministero dell'Istruzione, dell'Università e della Ricerca ha profuso un grosso impegno negli ultimi anni nel promuovere le politiche del cosiddetto **"Better Internet for Kids**" attraverso le iniziative nell'ambito del Piano Nazionale Scuola Digitale e delle Linee di Orientamento per Azioni di Prevenzione e Contrasto al Bullismo e al Cyberbullismo. Tali iniziative hanno trovato un importante fattore di consolidamento nell'implementazione del progetto ***"Generazioni Connesse"*** nel quale si traduce sostanzialmente l'azione del **Safer Internet Centre Italiano**, co-finanziato dalla Commissione Europea nell'ambito del programma Connecting Europe Facility (CEF) - Telecom, e membro di una rete di Safer Internet Centre presenti in tutta Europa, coordinata da INSAFE e Inhope (https://www.betterinternetforkids.eu/).

Il Safer Internet Centre (noto anche come SIC) nasce per fornire informazioni, consigli e supporto a bambini/e, ragazzi/e, genitori, docenti ed educatori che hanno esperienze anche problematiche riguardo la Rete. Le iniziative del MIUR hanno fornito un contribuito all'allineamento dell'Agenda Digitale Italiana con le Comunicazioni e le Raccomandazioni UE. Il Safer Internet Centre, in particolare, si presenta come punto di riferimento a livello nazionale delle iniziative per la sensibilizzazione, la prevenzione e l'educazione ALL'USO POSITIVO DELLE TECNOLOGIE DIGITALI E LA PREVENZIONE DEI RISCHI NELLE SCUOLE.

In questo quadro rientra anche l'attivazione **dell'Advisory Board** come organismo di consultazione che ha offerto al MIUR e al Safer Internet Centre l'occasione per avviare una concertazione inter-istituzionale allargata alle principali aziende delle Tecnologie dell'Informazione e della Comunicazione (TIC), alle associazioni, organizzazioni, enti e ai più diffusi social network per la messa in opera di una sinergica e fattiva collaborazione tra le iniziative per l'educazione alla sicurezza in Rete.

- Finalità e target delle Linee Guida

Negli ultimi anni si sono moltiplicate le azioni, le attività, i progetti realizzati da istituzioni, organizzazioni e aziende all'interno delle scuole che hanno coinvolto in maniera diretta studenti/studentesse ed insegnanti.

Tali attività sono state rilevate sul territorio nazionale attraverso una **"SURVEY"** che ha tracciato una prima mappatura del tipo di attività svolta, degli obiettivi perseguiti e dei risultati raggiunti.

I risultati dell'indagine hanno evidenziato la necessità di indicazioni che possano aumentare la qualità e la tracciabilità degli interventi nel settore. L'obiettivo del presente documento è quello di fornire dei principi guida ai quali attenersi per la realizzazione di iniziative nelle scuole, finalizzate a promuovere un uso positivo e consapevole delle Tecnologie Digitali da parte dei più giovani, e/o finalizzate a prevenire e contrastare situazioni di rischio online. Tali principi intendono rappresentare degli standard di qualità minimi da osservare da parte di attori pubblici e privati che realizzano iniziative nelle scuole con i fini sopra indicati.

- I contenuti delle Linee Guida

I contenuti delle seguenti linee guida indicano alcuni approcci psico-pedagogici e comportamentali da adottare negli interventi da realizzare nelle scuole, quale risultato dell'esperienza maturata in seno a Generazioni Connesse in collaborazione con **l'Advisory Board**. I contenuti sono suddivisi nelle seguenti 7 aree:

1. L'adozione di una strategia integrata e globale;
2. L'adozione di una politica di prevenzione;
3. La segnalazione e presa in carico di situazioni potenzialmente a rischio;
4. La valutazione dei bisogni e la definizione degli obiettivi;
5. L'approccio metodologico;
6. La valutazione degli interventi al fine di promuovere pratiche di comprovata efficacia;
7. La protezione dei dati personali.

1. ADOZIONE DI UNA STRATEGIA INTEGRATA E GLOBALE

1.1. Coinvolgimento di tutti gli attori della scuola: studenti e studentesse, docenti, genitori, e personale ATA, per l'affermazione di un modello di scuola come comunità.

1.2 Promozione dell'alleanza educativa tra scuola e famiglia: migliorare il livello di sensibilizzazione e comunicazione sull'importanza e la qualità del patto di corresponsabilità educativa tra scuola e famiglie, inserendo il tema delle Tecnologie Digitali.

1.3 Sviluppo e adozione del documento programmatico (e-policy) che definisca: a) l'approccio alle tematiche legate alle competenze digitali, alla sicurezza online e ad un uso positivo delle tecnologie digitali nella didattica; b) le norme comportamentali e le procedure per l'utilizzo delle tecnologie digitali in ambiente scolastico; c) le misure per la prevenzione e per la rilevazione e gestione delle problematiche connesse ad

un uso non consapevole delle tecnologie digitali.

1.4 Sviluppo di un curricolo digitale verticale e trasversale che diventi parte integrante della proposta formativa della scuola. Il curricolo digitale è costruito dalle proposte di tutto il corpo docente volte ad inserire nel proprio programma didattico temi, strumenti e prassi inerenti alle nuove tecnologie.

1.5 Inserimento del percorso dedicato e delle sue finalità all'interno del PTOF, in coerenza con il curriculo scolastico e quindi in applicazione delle Indicazioni Nazionali inerenti agli specifici percorsi di studio.

1.6 Promozione di conoscenze specifiche rivolte a tutti gli attori scolastici (insegnanti, studenti e genitori) in merito all'uso delle tecnologie digitali attraverso metodologie formative attive e partecipative che consentano anche processi di apprendimento orizzontale fra pari (peer to peer support) e di self/peer empowerment.

2. ADOZIONE DI UNA POLITICA DI PREVENZIONE

2.1 Messa in campo di azioni volte a intervenire prima della possibile insorgenza di comportamenti a rischio, che promuovano il benessere e l'uso sicuro e positivo delle tecnologie digitali per tutti gli attori della scuola a partire da quella primaria.

2.2. Promozione di interventi educativi e azioni a supporto di studenti e studentesse in caso di situazioni di cyberbullismo o di problematiche relative all'utilizzo della rete che coinvolgano tutti gli attori della scuola in linea con la legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo".

2.3 Progettazione e realizzazione di azioni e interventi che siano caratterizzati da multidisciplinarietà e alta qualificazione delle figure coinvolte.

2.4. In caso di interventi proposti da attori esterni alla scuola, preferenza per il contributo di professionalità diverse (es. educatori, psicologi, esperti informatici, polizia, etc …) che abbiano competenze sul tema delle tecnologie digitali e lavorino con obiettivi comuni, coordinati dalla scuola stessa.

2.5 Adozione di un sistema di tutela dei minori che coinvolga tutti gli attori pubblici e privati coinvolti in un percorso di formazione nelle scuole e che preveda misure preventive specifiche, come la sottoscrizione di un codice di condotta e di un'autocertificazione ai sensi dell'art.2 del D. Lgs. n.39/20141, da parte di tutti coloro (dipendenti, collaboratori, esperti, volontari) che abbiano contatti diretti con i minori.

3. SEGNALAZIONE E PRESA IN CARICO DI SITUAZIONI POTENZIALMENTE A RISCHIO

3.1 Creazione e implementazione di procedure per la segnalazione e gestione di problemi connessi a comportamenti a rischio online degli allievi/e: a) indirizzate internamente alla scuola, semplici e sostenibili, che prevedano una serie di figure di riferimento, tra le quali, gli insegnanti referenti per il contrasto del bullismo e del cyberbullismo; b) indirizzate all'esterno come procure, polizia postale, etc… per fattispecie di reati che lo prevedano e ai servizi del territorio per il supporto alle varie figure coinvolte.

3.2 Condivisione delle suddette procedure di segnalazione e gestione con tutti gli attori della scuola: docenti, personale ATA, genitori e studenti e studentesse con

modalità di volta in volta adeguate all'età.

4. VALUTAZIONE DEI BISOGNI E DEFINIZIONE DEGLI OBIETTIVI

4.1 Strutturazione degli interventi di prevenzione sulla base di una preliminare valutazione dei bisogni, delle necessità e delle conoscenze, competenze e capacità iniziali della popolazione target che beneficerà dell'intervento.

4.2 Definizione chiara degli obiettivi degli interventi. Possono essere rivolti a colmare lacune e/o a promuovere un cambiamento nelle conoscenze, nelle competenze, negli atteggiamenti o nei comportamenti.

4.3 Condivisione chiara e trasparente dei presupposti, degli obiettivi, delle procedure, dei risultati attesi con tutti gli attori della scuola.

5. APPROCCIO METODOLOGICO

5.1 Promozione dell'educazione al rispetto. Assunzione e promozione di un approccio basato sui diritti umani e sulla tutela della dignità umana, su un dialogo paritario e rispettoso tra tutti gli individui, che promuova il contrasto a messaggi di odio, violenza e discriminazione sia online sia nella dimensione reale.

5.2 Sviluppo del pensiero critico per un uso consapevole delle tecnologie digitali e della capacità di assumersi la responsabilità delle proprie azioni e delle proprie scelte nell'utilizzo di tali tecnologie.

5.3 Promozione dell'Educazione Civica Digitale, attraverso l'uso delle risorse messe a disposizione dal Curriculum di Educazione Civica Digitale, che aiuti ad una maggiore comprensione dei rischi e delle potenzialità degli ambienti digitali.

6. VALUTAZIONE DEGLI INTERVENTI AL FINE DI PROMUOVERE PRATICHE DI COMPROVATA EFFICACIA

6.1 Utilizzo di criteri di valutazione e monitoraggio che siano stati precedentemente definiti, esplicitati e condivisi in base ai quali si possa giudicare l'efficacia e l'impatto dell'intervento. I criteri devono essere definiti in base agli obiettivi dai quali derivano direttamente. Per monitoraggio e valutazione si intendono processi e strumenti sia "qualitativi" sia "quantitativi".

6.2 Preferenza per l'attuazione di programmi, percorsi, progetti e strumenti che siano già stati valutati e abbiano dimostrato di essere efficaci, in grado cioè di generare un cambiamento, rispondendo positivamente all'obiettivo che si erano prefissati di raggiungere (es. aumento delle conoscenze, diminuzione dei comportamenti a rischio, etc …).

6.3 Adattamento, trasferimento e implementazione nel nostro paese di buone pratiche che emergono a livello internazionale, cioè di programmi, percorsi, progetti e strumenti efficaci.

7. PROTEZIONE DEI DATI PERSONALI

7.1 Adeguamento delle informative finalizzate all'acquisizione del consenso genitoriale in relazione al trattamento dei dati personali delle persone minorenni al Regolamento Generale sulla Protezione dei Dati Personali.

7.2 Aggiornamento delle informative che devono essere scritte in modo comprensibile e devono contenere le seguenti informazioni:
- chi è il responsabile del trattamento dei dati personali delle persone minorenni, come vengono raccolti e dove vengono immagazzinati;
- con quali finalità i dati delle persone minorenni vengono raccolti (i dati devono sempre essere raccolti per finalità determinate, esplicite e legittime);
- se i dati personali delle persone minorenni vengono trasferiti in Paesi al di fuori dell'Unione Europea e, in caso affermativo, attraverso quali strumenti;
- se i dati personali delle persone minorenni vengono ceduti a terzi e, in caso affermativo, chi è il titolare;
- il tempo di conservazione dei dati delle persone minorenni e i criteri seguiti per stabilire tale periodo di conservazione;
- se ed in che modo i dati personali inesatti delle persone minorenni possono essere rettificati e/o cancellati.

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 Dirigente Scolastica deve:

- Garantire la corretta formazione del personale scolastico sulle tematiche relative all'uso sicuro e consapevole della Rete
- Garantire una formazione adeguata del personale docente relativa all'uso delle TIC nella didattica e che le modalità di utilizzo sicuro e corretto delle stesse siano integrate nel curriculum di studio e nelle attività didattico-educative dei discenti
- Verificare l'effiicacia del sistema di monitoraggio e controllo interno della sicurezza online
- Osservare le procedure, previste dalle norme, in caso di reclami o attribuzione di responsabilità al personale scolastico, in relazione ad incidenti occorsi agli alunni nell'utilizzo delle TIC

L'Animatrice digitale, supportata dal TEAM per l'innovazione, deve:

- Promuovere la formazione interna all'Istituzione negli ambiti di sviluppo della "scuola digitale"; fornire consulenza e informazioni al personale sui rischi online ed alle misure di prevenzione e gestione degli stessi
- Monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e delle rete

- Proporre la revisione delle politiche dell'Istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili
- Assicurare agli utenti l'accesso alla rete esclusivamente tramite password applicate e regolarmente modificate
- Curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti
- Coinvolgere la comunità scolastica nella partecipazione ad attività e progetti funzionali alla sviluppo di una cittadinanza digitale attiva

La referente del bullismo e cyberbullismo deve:

- Coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo
- Coinvolgere con attività di formazione e progetti la comunità educante ed i genitori dei discenti

La Direttrice dei Servizi Generali e Amministrativi deve:

- Assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento dei tecnici al fine di garantire la funzionalità dell'infrastruttura tecnica, la sicurezza della stessa da un uso improprio o dannosi attacchi esterni
- Garantire il funzionamento dei molteplici canali di comunicazione all'interno della scuola e tra la stessa e le famiglie per le notifiche relative all'utilizzo delle tecnologie digitali e della rete

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 capiscano 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, etc ... 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'Animatrice 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 alla Dirigente Scolastica 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 dalle norme

I discenti devono:

- Essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti
- Avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore
- Comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi
- Adottare condotte rispettose degli altri anche quando si comunica in rete
- Esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori

I genitori devono:

- Sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica
- Seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di internet
- Concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet
- Fissare delle regole per l'utilizzo dei dispositivi e della rete e controllarne l'uso

Gli Enti esterni e le Associazioni 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

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

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

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

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

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

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

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

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

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

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

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

1. Condividere e comunicare la politica di e-safety agli alunni

Tutti gli alunni saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati soltanto previa autorizzazione degli stessi.

L'istruzione degli alunni riguardo all'uso responsabile e sicuro di internet precederà l'accesso alla rete.

L'elenco delle regole per la sicurezza on-line sarà pubblicato in tutte le aule o laboratori con accesso a internet.

Nell'educazione sulla sicurezza sarà dato particolare rilievo agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più "vulnerabili".

2. Condividere e comunicare la politica di e-safety al personale

La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet sarà oggetto di discussione da parte degli organi collegiali e comunicata formalmente a tutto il personale con il presente documento e altro

materiale informativo anche 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 limitato 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 on-line del personale docente nell'uso sicuro e responsabile di internet, sia professionalmente che personalmente, sarà fornita anche attraverso il sito web della scuola.

Il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC, sarà supervisionato dall'Animatrice digitale che segnalerà alla DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici.

L'Animatrice digitale metterà in evidenza on-line utili strumenti 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.

3. Condividere e comunicare la politica di e-safety ai genitori

L'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di internet sarà attirata in aree specifiche del sito web della scuola;

Sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali.

L'Animatrice digitale fornirà ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di internet anche a casa.

L'Animatrice digitale e i docenti di classe forniranno ai genitori indirizzi sul web relativi a risorse utili per lo studio e a siti idonei ed educativi per gli alunni, sistemi di filtraggio e attività formative per il tempo libero.

1.5 - Gestione delle infrazioni alla ePolicy

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

1. Disciplina dei discenti

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

- un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare; l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;

- la condivisione di immagini intime o troppo spinte; la comunicazione incauta e senza permesso con sconosciuti;

- 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.

Sono previsti pertanto da parte dei docenti provvedimenti "disciplinari" proporzionati all'età e alla gravita dell'infrazione, 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. 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.

2. Disciplina del personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico e, in particolare, i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet, sono diverse e alcune possono determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli alunni:

- Un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli

alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite installazione di software o il salvataggio di materiali non idonei;
- Un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- Un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi; una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- Una carente istruzione preventiva degli alunni sull'utilizzazione corretta e responsabile delle tecnologie digitali e di internet;
- Una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- Insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, alla Dirigente scolastica, all'Animatrice digitale;
- La Dirigente Scolastica può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone una copia per eventuali successive investigazioni;
- Tutto il personale è tenuto a collaborare con la Dirigente scolastica e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo, gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse;
- Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

3. Disciplina dei genitori

- In considerazione dell'età degli alunni e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico;
- Le situazioni familiari meno favorevoli sono: a) la convinzione che il proprio figlio a casa possa utilizzare i supporti informatici in modo corretto; b) una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio; c) una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone; d) un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei; e) un utilizzo del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria indirizzi o contenuti non idonei;
- I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla

gravità dei comportamenti dei loro figli,se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

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.

La policy richiede l'integrazione con l'inserimento delle seguenti norme: a) Le apparecchiature presenti nella scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto; b) Le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente; c) In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile; d) In caso di malfunzionamento non risolvibile dal responsabile di laboratorio, il suddetto contatterà la segreteria e poi il tecnico.

In ogni caso si rinvia al Regolamento relativo all'utilizzo delle TIC, pubblicato sul sito della scuola.

Disposizioni sull'uso dei software

1. I software installati sono ad esclusivo uso didattico

2. In base alle leggi che regolano la distribuzione delle licenze, i prodotti software presenti in laboratorio non sono disponibili per il prestito individuale

3. E' fatto divieto di usare software non conforme alle leggi sul copyright. E' cura dell'insegnante utente di verificarne la conformità. Gli insegnanti possono installare nuovo software sui PC del laboratorio della propria scuola, previa autorizzazione scritta del Dirigente Scolastico solo se il software installato rispetta le leggi sul copyright

4. E' responsabilità degli insegnanti che chiedono al Responsabile di laboratorio di effettuare copie per uso didattico, di assicurarsi che la copia non infranga le leggi sul copyright in vigore

Accesso a internet

1. L'accesso a Internet è consentito solo ad esclusivo uso didattico e/o di formazione

2. Internet non può essere usato per scopi vietati dalla legislazione vigente

3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet

4. E' vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza. Norme finali Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

Si riporta l'art. 49 del Regolamento di Istituto relativo a "UTILIZZO DEL TELEFONO CELLULARE E DEI VARI DISPOSITIVI ELETTRONICI DURANTE LE ATTIVITÀ SCOLASTICHE" *a) Salvo casi del tutto eccezionali, i telefoni cellulari non devono essere portati a scuola e non devono comunque essere utilizzati durante l'orario scolastico. Se – malgrado il divieto – gli studenti verranno sorpresi ad usare il cellulare, lo stesso verrà temporaneamente requisito dai docenti che registreranno l'episodio sul registro di classe e – in collaborazione con il personale ausiliario e/o con la segreteria – convocheranno per le vie brevi i genitori interessati ai quali verrà riconsegnato il cellulare requisito. Avuto inoltre riguardo per il fatto che i moderni cellulari possono essere utilizzati anche per scattare foto (o effettuare riprese filmate) e per trasferirle con un MMS, si informano i Sigg. genitori che eventi di questo tipo – se si concretizzano durante l'orario scolastico – si possono configurare anche come reati per i quali non si esclude la segnalazione ai competenti organi di Pubblica Sicurezza. b) L'Istituzione Scolastica non ha e comunque non si assume alcuna responsabilità né relativamente all'uso improprio o pericoloso che gli studenti dovessero fare del cellulare (es.: inviare/ricevere messaggi a/da soggetti ignoti agli stessi genitori), né relativamente a smarrimenti e/o 'sparizioni'di telefonini cellulari o di lettori mp3 o di hard/disk portatili o pen drive. c) In ogni caso, i genitori tengano conto che le comunicazioni urgenti ed improcrastinabili possono essere trasmesse ai loro figli durante l'orario scolastico rivolgendosi telefonicamente alle singole sedi scolastiche ovvero in Segreteria. d) Il divieto ribadito per i telefoni/videotelefoni cellulari e per i lettori mp3 si estende ovviamente anche ad altri oggetti il cui uso a scuola può persino arrecare danni a terzi. e) La scuola non pone alcun ostacolo all'utilizzo di cd/dvd rom o di hard - disk portatili come strumenti di lavoro e di studio. Ciò che a riguardo compete alle famiglie è il controllo periodico del contenuto di questi strumenti per evitare che qualche studente 'trasporti' a scuola immagini / testi / filmati per così dire 'sconvenienti', avendoli scaricati. Per impedire che le stesse postazioni dei laboratori scolastici possano essere furtivamente utilizzate per visitare siti volgari e pericolosi, la scuola si è da tempo dotata di un software di sicurezza che filtra gli accessi ad internet e protegge quindi i visitatori meno esperti. Oltre a questo sofisticato sistema di protezione che blocca l'accesso ai siti di cui si discorre, la scuola ovviamente mette in campo soprattutto la vigile attenzione educativa di ogni singolo docente. f) Fermo restando il fatto che la scuola è un'istituzione educativa e che non è né prevista, né possibile, né tantomeno legittima la perquisizione quotidiana di tutti gli*

studenti all'inizio di ogni giorno di lezione, le responsabilità che dovessero derivare dal verificarsi di eventi riconducibili all'uso non corretto o non legittimo di uno qualsiasi degli oggetti di cui alla presente norma regolamentare sono tutte ascrivibili alle famiglie degli studenti eventualmente coinvolti. Le responsabilità appena menzionate sono condivise dal personale scolastico solo quando e solo se – avendo personalmente constatato o essendo venuto a conoscenza che qualche ragazzo/a ha con sé durante l'orario scolastico un oggetto potenzialmente pericoloso e/o il cui uso può compromettere la serenità del clima interno alla scuola non dovesse immediatamente intervenire nelle forme già indicate e comunque in modo tale da prevenire o reprimere sul nascere situazioni incompatibili con le più elementari regole della civile convivenza.

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'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy
- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti
- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto per la stesura finale dell'ePolicy
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti

- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai genitori

Azioni da svolgere nei prossimi 3 anni:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy
- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti
- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell'Istituto per la stesura finale dell'ePolicy
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto 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.

La costruzione del curricolo digitale di Istituto si presenta come strumento per lo sviluppo delle competenze digitali dei nostri studenti e come esigenza inderogabile di offrire loro una nuova dimensione di cittadinanza attiva e consapevole. Dalla "Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente", C189/9, p.9, maggio 2018 è individuata la definizione, che sta alla base del presente documento, di competenza digitale: "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 «nativo digitale» significa nascere in una società permeata di comunicazione digitale**).
Pertanto, il "nativo digitale" che si introduce da solo nella comunicazione

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

LA SCUOLA DEVE GUIDARLO ED ISTRUIRLO IN QUESTO AMBIENTE IMMERSIVO IN CUI VIVE, nei tempi e nei modi più consoni all'età e alla propria personale propensione all'interazione in rete.

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

Leggiamo inoltre dal PROFILO DELLO STUDENTE AL TERMINE DEL PRIMO CICLO DI ISTRUZIONE (Indicazioni Nazionali 2012): "*L'alunno ha buone competenze digitali, usa con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati e informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo.*"

La competenza digitale è stata recentemente inserita dal Consiglio dell'Unione Europea nel novero delle competenze di base, accanto a quelle alfabetiche e matematiche.

Purtroppo, come confermano i dati del *Digital Economy and Society Index*, il nostro sistema-Paese presenta profonde debolezze in questo campo, particolarmente gravi proprio nel campo della competenza digitale dei cittadini, che va quindi coltivata e potenziata in modo efficace e coerente durante l'intero percorso scolastico.

Il nostro Istituto, in perfetta sintonia con le indicazioni provenienti dal Consiglio Europeo e dal MIUR, ha predisposto il presente curricolo, definendo i traguardi formativi per la scuola del I Ciclo.

Un Curricolo Digitale con forti elementi di interdisciplinarità e trasversalità curricolare, declinato attraverso modalità di apprendimento pratico e sperimentale, metodologie e contenuti a carattere innovativo, teso ad accelerare e aumentare l'impatto verso il rinnovamento delle metodologie didattiche.

Le DIMENSIONI DELLE COMPETENZE DIGITALI, come già evidente nella definizione iniziale delle Raccomandazioni Europee, sulle quali sarà possibile lavorare in classe, *in un'ottica che integra la dimensione tecnologica con quella cognitiva ed etica* (Calvani, Fini e Ranieri, 2009) sono:

- dimensione **TECNOLOGICA**: è importante far riflettere i più giovani sul potenziale delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana, onde evitare automatismi che abbiano conseguenze incerte, attraverso un'adeguata comprensione della "grammatica" dello strumento
- dimensione **COGNITIVA**: fa riferimento alla capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità
- dimensione **ETICA E SOCIALE**: la prima fa riferimento alla capacità di gestire in modo sicuro i propri dati personali e quelli altrui, e di usare le tecnologie digitali per scopi eticamente accettabili e nel rispetto degli altri. La seconda, invece, pone un po'

più l'accento sulle pratiche sociali e quindi sullo sviluppo di particolari abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di coloro con cui comunichiamo online.
Le CINQUE AREE delle COMPETENZE DIGITALI, in riferimento al DIGCOMP 2.1. (Quadro comune di riferimento europeo per le competenze digitali), sono:
1. ALFABETIZZAZIONE E DATI: identificare, localizzare, recuperare, conservare, organizzare e analizzare le informazioni digitali, giudicare la loro importanza e lo scopo
2. COMUNICAZIONE E COLLABORAZIONE: comunicare in ambienti digitali, condividere risorse attraverso strumenti on-line, collegarsi con gli altri e collaborare attraverso strumenti digitali, interagire e partecipare alle comunità e alle reti
3. CREAZIONE DI CONTENUTI DIGITALI: creare e modificare nuovi contenuti (da elaborazione testi a immagini e video); integrare e rielaborare le conoscenze e i contenuti; produrre espressioni creative, contenuti media e programmare; conoscere e applicare i diritti di proprietà intellettuale e le licenze
4. SICUREZZA: protezione personale, protezione dei dati, protezione dell'identità digitale, misure di sicurezza, uso sicuro e sostenibile
5 PROBLEM-SOLVING: identificare i bisogni e le risorse digitali, prendere decisioni informate sui più appropriati strumenti digitali secondo lo scopo o necessità, risolvere problemi concettuali attraverso i mezzi digitali, utilizzare creativamente le tecnologie, risolvere problemi tecnici, aggiornare la propria competenza e quella altrui.

I livelli di competenza declinati sono 6, differentemente dagli otto livelli di competenza presenti nel quadro di riferimento: essi sono da ricondurre ai traguardi di competenza al termine della scuola primaria (base 1, 2 e intermedio 3) e al termine della scuola secondaria di primo grado (intermedio 4, avanzato 5, 6).
Per una esaustiva esposizione di detti livelli, si rimanda al documento allegato al presente.

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.

Gli insegnanti devono raggiungere un buon livello di formazione in merito all'utilizzo e all'integrazione delle TIC nella didattica. L'Istituto, attraverso il Collegio del Docenti, riconosce e favorisce la partecipazione del personale ad iniziative promosse sia dalla scuola, dalle Reti di scuole, dall'Amministrazione, sia da quelle scelte liberamente dai docenti, purchè coerenti con il piano di formazione. Fondamentale porre attenzione all'uso del TIC nella didattica: un loro utilizzo strutturato e integrato rende gli apprendimenti motivanti, coinvolgenti ed inclusivi e permette al docente di guidare studenti e studentesse nella fruizione dei contenuti online, sempre più importante anche in ambito lavorativo (lavoro di gruppo anche a distanza, confronto fra pari in modalità asincrona).

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.

I momenti di formazione e aggiornamento saranno progettati sulla scorta :

- dell'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica;
- dell'analisi del fabbisogno conoscitivo circa particolari argomenti che si sentono come più cogenti per i docenti e l'Istituto;
- dell'analisi delle richieste che provengono dagli studenti e dalle studentesse in modo, poi, da riutilizzarli nel loro lavoro di educatori (attraverso le modalità che il docente indica e ritiene più confacente alla classe) quanto appreso durante la formazione ricevuta.

Sarà elaborato un cronoprogramma triennale che preveda azioni specifiche quali:

Analizzare il fabbisogno formativo degli insegnanti sull'uso sicuro della Rete;

- Promuovere la partecipazione dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto “Generazioni Connesse”.
- Monitorare le azioni svolte per mezzo di specifici momenti di valutazione;
- Organizzare incontri con professionisti della scuola o con esperti esterni, enti/associazioni.

Sarà predisposta un’area specifica sul sito dell’Istituto con materiali formativi per gli insegnanti. Documento di e-policy

Nella sezione, saranno messi a disposizione materiali per l’aggiornamento sull’utilizzo consapevole e sicuro di Internet, prevedendo possibilità e modalità di condivisione fra gli insegnanti.

Sul sito istituzionale della scuola, è presente il link a Generazioni Connesse, attraverso cui accedere alla fruizione di materiale informativo con approfondimenti, spunti aggiornamenti e strumenti didattici utili da usare con gli studenti e le studentesse, per ciascun grado di scuola.

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

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

Il Patto di Corresponsabilità verrà adattato con indicazioni volte a sensibilizzare le famiglie.

Il nostro piano d'azioni

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

Verrà sviluppata almento una delle seguenti azioni:

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo 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.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

Verrà sviluppata almeno una delle seguenti azioni:

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo 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.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare

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

Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc. Fra questi, particolarmente importanti sono: i dati che permettono l'identificazione diretta di una persona, come i dati anagrafici (ad es. nome e cognome); i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad es. il codice fiscale, l'indirizzo IP, il numero di targa); i dati rientranti in particolari categorie: si tratta dei dati cosiddetti sensibili, cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale di una persona. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale; i dati relativi a condanne penali e reati: si tratta dei dati cosiddetti giudiziari, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad es. i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto o obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza. I soggetti sono: L'interessato, che è la persona fisica alla quale si riferiscono i dati personali (art. 4, paragrafo 1, punto 1), del Regolamento UE 2016/679); Il titolare, che è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico, privato o l'associazione che adotta le decisioni sugli scopi e sulle modalità del trattamento (art. 4, paragrafo 1, punto 7), del Regolamento UE 2016/679); Il responsabile , che è la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo del trattamento dei dati (art. 4, paragrafo 1, punto 8), del Regolamento UE 2016/679). Il Regolamento medesimo ha introdotto la possibilità che un responsabile possa, a sua volta e secondo determinate condizioni, designare un altro soggetto c.d. sub-responsabile (art. 28, paragrafo 2). Trattamento dei dati è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali o insiemi di dati personali. Ad esempio: la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, par. 1, punto 2, del Regolamento (UE) 2016/679). I soggetti che procedono al trattamento dei dati personali altrui devono adottare particolari misure per garantire il corretto e sicuro utilizzo dei dati.

Il nostro Istituto Il nostro Istituto Scolastico in conformità al al Regolamento UE 2016/679 deve:

Redigere e mantenere un registro dei trattamenti dei dati: sia per il titolare che per il responsabile dei trattamenti. Valutare i rischi sulla privacy: (definita nel regolamento Data Protection Impact Assessment o PIA) relativamente ad alcune tipologie di trattamento dei dati sensibili.

Le istituzioni scolastiche pubbliche e private possono trattare anche dati sensibili, come ad esempio dati relativi alle origini razziali per favorire l'integrazione di alunn*, dati relativi alle convinzioni religiose, al fine di garantire la libertà di culto, e dati relativi alla salute per adottare misure di sostegno di alunn*, come i dati vaccinali con le Asl.

Analizzare il processo sulla raccolta/gestione del consenso: occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2).

Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice e chiara (art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali, ma devono ad esempio adeguare tutta la modulistica al Regolamento UE 2016/679 e predisporre una lettera di incarico per il trattamento dei dati al personale ATA, ai collaboratori scolastici e ai docenti.

Adottare idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti: analisi del sito web istituzionale di riferimento con proposte volte a migliorare la sicurezza e la protezione dei dati trattati proposte in messa in sicurezza della intranet scolastica sulle reti Wi-fi installate.

Utilizzare un firewall hardware.

Istituire corsi di formazione destinati ai responsabili, agli incaricati ed eventualmente ai subincaricati del trattamento. Relativamente ai corsi di formazione, tali tematiche verranno - altresì - suggerite alla scuola polo per la formazione d'ambito.

3.2 - Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*

3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

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

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

L'IC "*CARINI-CALDERONE -TORRETTA*" dispone dell'accesso alla rete *wi-fi* in gran parte dei Plessi. La rete è dotata di un *firewall* per la prevenzione dagli accessi dall'esterno nonché di filtri dei contenuti attraverso l'utilizzo di blacklist e parole chiave in continuo aggiornamento.

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.

Tutti i docenti dell'istituto possiedono una e-mail della scuola: nomecognome@iccalderone.edu.it.

Gli alunni, per l'utilizzo delle attività didattiche in Flipped e per la DaD sono dotati di un indirizzo di posta elettronica della scuola: nome.cognome@iccalderone.edu.it.
La dotazione di indirizzi di posta elettronica sia dei docenti che degli alunni appartiene all'infrastruttura delle Google Suite for Education.

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 sito *web* della scuola è gestito da un team preposto che si adopera affinché il sito sia sicuro e accessibile; ha cura di effettuare sia aggiornamenti e backup periodici che intervenire in caso di emergenza.

Il nostro piano d'azioni

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

Verrà sviluppata almento una delle seguenti azioni:

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte deglistudenti e delle studentesse.
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti.
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA.
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto perredigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola.
- Organizzare incontri per la consultazione degli studenti/studentesse suindicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola.
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamentisull'uso dei dispositivi digitali personali a scuola.
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare 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).

Verrà sviluppata almeno una delle seguenti azioni:

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

parte delpersonale Tecnico Amministrativo e dagli ATA.

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto perredigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione degli studenti/studentesse suindicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamentisull'uso dei dispositivi digitali personali.
- Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare 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.*

In conformità alla normativa vigente l'IC "*CARINI-CALDERONE –TORRETTA*" ha:
Nominato **una referente** che si occupa della prevenzione e del contrasto del bullismo e cyberbullismo.
Redatto e approvato un regolamento contro il bullismo-cyberbullismo, pubblicato sul sito web della scuola, sia nella sezione Regolamenti sia nella sezione "*Stop al*

Bullismo".
Il regolamento include, anche, una parte dedicata all'uso di Internet in cui gli studenti si impegnano a:
- utilizzare la rete nel modo corretto
- non scaricare materiali e software senza autorizzazione e non utilizzare unità removibili personali senza autorizzazione
- tenere sempre spento lo smartphone salvo nei casi in cui ciò sia consentito

Nel regolamento sono indicate anche le modalità di segnalazione di presunti episodi di bullismo/cyberbullismo nonché ogni utile elemento per alunn*, docenti, famiglie.

Le tipologie di cyberbullismo maggiormente considerate sono:
Hate speech (il fenomeno dell'incitamento all'odio, all'intolleranza verso un gruppo o una persona.
Dipendenza da internet e dal gioco o-nline (i comportamenti patologici/dipendenze).
Sexting (scambio di contenuti mediali sessualmente espliciti).
Grooming o adescamento online (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).
Denigration (diffusione di pettegolezzi, insulti, voci lesivi della dignità della persona).
Body shaming (prendere in giro per l'aspetto fisico).

Nei paragrafi successivi tali forme di bullismo verranno analizzate nel dettaglio.

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).

Si rinvia, in ogni caso, al Regolamento di Istituto per la prevenzione dei fenimeni del Bullismo e del Cyberbullismo pubblicato nella sezione "Stop al Bullismo" del sito www.iccalderone.edu.it

---

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.

Il nostro Istituto porrà in essere tutte le azioni finalizzate a prevedere e prevenire tale fenomeno.

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?

L'Istituto ha già posto in essere delle attività, in collaborazione con esperti esterni, finalizzati alla prevenzione del fenomeno della ludopatia (si pensi alla campagna "Io, giovane attore" che ha quale slogan "scegliamo il gioco che fa bene alla salute). Tale attività verrà riproposta anche per i successivi anni scolastici tenuto conto dell'alta valenza educativa.

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.

Il nostro Istituto porrà in essere tutte le azioni finalizzate a prevedere e prevenire tale fenomeno.

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.

Il nostro Istituto porrà in essere tutte le azioni finalizzate a prevedere e prevenire tale fenomeno.

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.

Il nostro Istituto porrà in essere tutte le azioni finalizzate a prevedere e prevenire tale fenomeno.

Il nostro piano d'azioni

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

Verrà sviluppata almeno una delle seguenti azioni:

□ 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.

□ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

□ Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

□ Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

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

Verrà sviluppata almeno una delle seguenti azioni azioni:

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

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

studenti/studentesse.

□ Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.

□ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

□ Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

- **Cyberbullismo**: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le 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.

Strumenti a disposizione di student*

Al fine di guidare e sostenere student* nelle segnalazioni di eventuali situazioni problematiche vissute in prima persona o di cui sono testimoni, **l'Istituzione scolastica, si ribadisce,** prevede i seguenti strumenti:
- un indirizzo e-mail specifico per le segnalazioni e una scatola/box per la raccolta di segnalazioni anonime da inserita in uno spazio accessibile e ben visibile della scuola, al piano della segreteria
- sportello di ascolto con professionisti (operatrici psicopedagogiche dell'Osservatorio per la Dispersione scolastica)
- docente referente per le segnalazioni.

La scheda di segnalazioni degli episodi di bullismo/cyberbullismo è, altresì, disponibile nella sezione "Stop al Bullismo" del sito web della scuola.

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.

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.

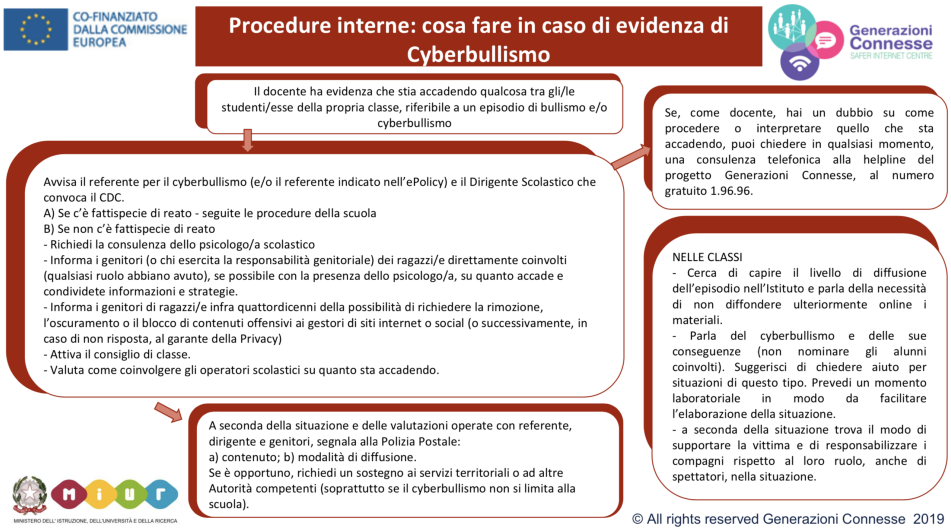
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

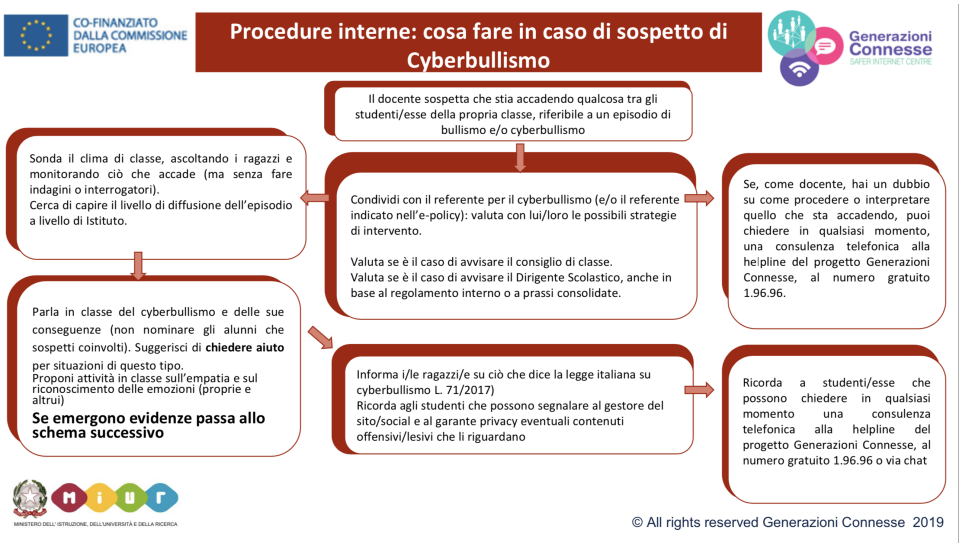
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare 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.

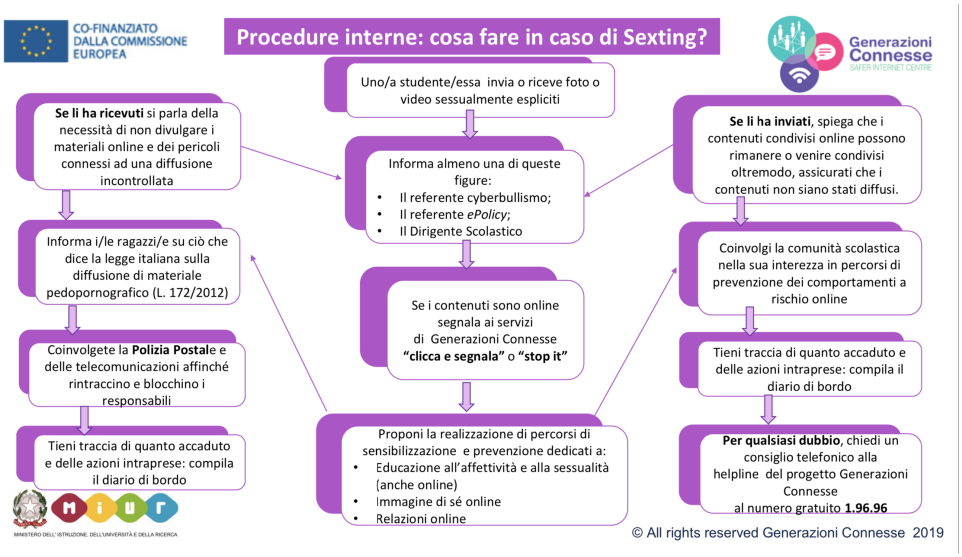
5.4. - Allegati con le procedure

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

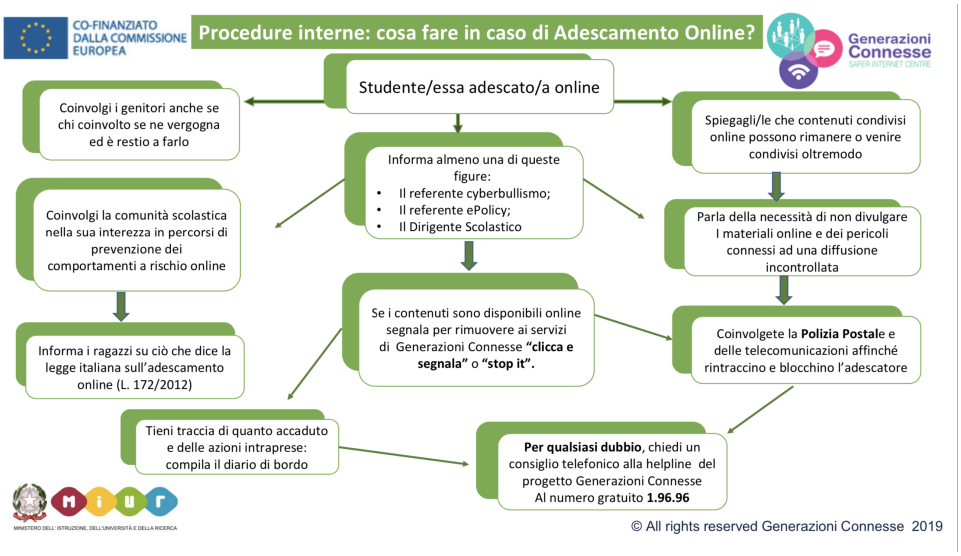




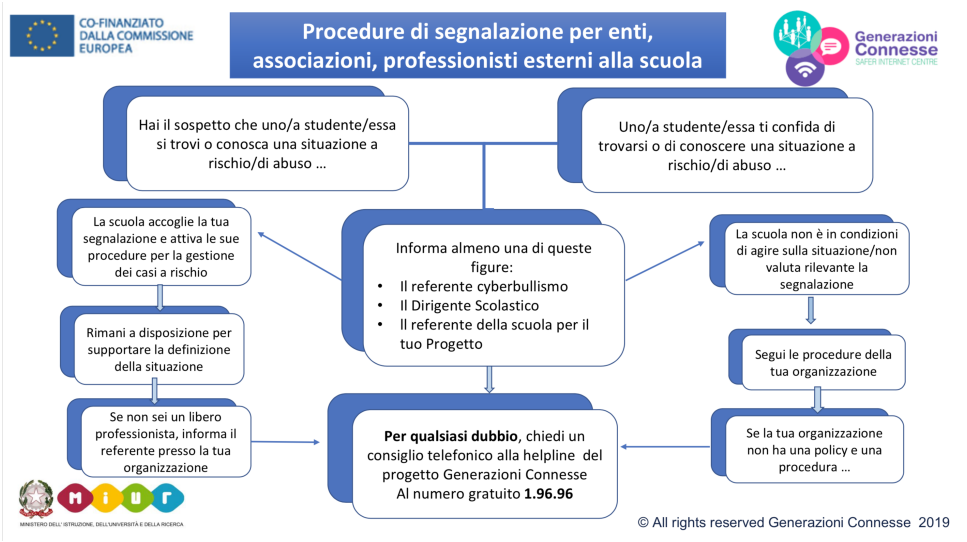
Procedure interne: cosa fare in caso di sexting?



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

Il nostro piano d'azioni

Il Piano di azione verrà implementato, come atto di integrazione al Piano Triennale dell'Offerta formativa dell'Istituzione Scolastica, per l'a.s. 2021/2002.