



Documento di ePolicy

CEIC84500L

I.A.C."D.CIMAROSA" AVERSA

VIA PAOLO RIVERSO 27 - 81031 - AVERSA - CASERTA (CE)

MARIO AUTORE

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

1. Presentazione dell'ePolicy

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

5. Gestione delle infrazioni alla ePolicy
 6. Integrazione dell'ePolicy con regolamenti esistenti
 7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
- 2. Formazione e curriculum**
1. Curriculum sulle competenze digitali per gli studenti
 2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
 3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
 4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
- 3. Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
1. Protezione dei dati personali
 2. Accesso ad Internet
 3. Strumenti di comunicazione online
 4. Strumentazione personale
- 4. Rischi on line: conoscere, prevenire e rilevare**
1. Sensibilizzazione e prevenzione
 2. Cyberbullismo: che cos'è e come prevenirlo
 3. Hate speech: che cos'è e come prevenirlo
 4. Dipendenza da Internet e gioco online
 5. Sexting
 6. Adescamento online
 7. Pedopornografia
- 5. Segnalazione e gestione dei casi**
1. Cosa segnalare
 2. Come segnalare: quali strumenti e a chi
 3. Gli attori sul territorio per intervenire
 4. Allegati con le procedure

Perché è importante dotarsi di una E-policy?

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

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

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.

Ruoli e Responsabilità (che cosa ci si aspetta da tutti gli attori della Comunità Scolastica).

Dirigente scolastico: Il ruolo del Dirigente scolastico nel promuovere l'uso consentito delle tecnologie e di internet include i seguenti compiti:

- I dirigenti scolastici sono chiamati a effettuare misure di intervento immediato qualora vengano a conoscenza di episodi di cyberbullismo e dovranno essere integrate e previste nei Regolamenti di Istituto e nei Patti di Corresponsabilità;
- Sarà cura del dirigente assicurare la massima informazione alle famiglie di tutte le attività e iniziative intraprese, anche attraverso una sezione dedicata sul sito web della scuola, che potrà rimandare al sito del MIUR www.generazioniconnesse.it
- è auspicabile che il dirigente scolastico attivi specifiche intese con i servizi territoriali (servizi della salute, servizi sociali, forze dell'ordine, servizi minorili dell'amministrazione della Giustizia) in grado di fornire supporto specializzato e continuativo ai minori coinvolti ove la scuola non disponga di adeguate risorse;
- garantire che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della comunicazione (TIC);
- condividere e seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola;
- A tale scopo necessita di ricevere tempestive informazioni sulle violazioni al presente regolamento o eventuali problemi di cui può venire a conoscenza il corpo docente o il personale ATA ;

Animatore digitale:

- stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- relazionarsi con la ditta che gestisce l'assistenza tecnico-informatica per definire le misure di sicurezza informatica più opportune;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curarne la manutenzione ;

- condividere la E-Safety Policy sul sito della scuola;
- controllare (una tantum e/o all'evenienza di episodi dubbi) del sistema informatico (cronologia, cookies, ecc.) da parte dei responsabili;
- installare firewall sull'accesso Internet
- aggiornare periodicamente i software antivirus e scansionare le macchine in caso di sospetta presenza di virus;

DSGA

- assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;
- garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.

Docente referente

- Il docente referente 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).
- 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;
- assicurare che l'educazione alla sicurezza online sia incorporata in tutto il programma di studi;
- promuovere la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica;
- promuovere la formazione e dare consulenza a tutto il personale;
- promuovere attività o progetti da svolgere nelle classi;
- applicare e controllare i protocolli di rilevazione, monitoraggio e gestione delle potenziali azioni di cyber bullismo;
- diffondere la E- Safety Policy attraverso power point e schede semplificate;
- collaborare con tutte le agenzie educative e istituzionali (associazioni sportive, polizia postale, associazioni di sostegno, etc.) per prevenire e gestire i casi di possibile cyber bullismo;
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti l'utilizzo consapevole di internet.

Il personale scolastico (ata, segreteria, etc)

- essere consapevoli dei problemi di sicurezza on-line connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili;
- comprendere e contribuire a promuovere politiche di e-sicurezza ;
- monitorare l'uso di dispositivi tecnologici e attuare politiche scolastiche per quanto riguarda

questi dispositivi;

- segnalare qualsiasi abuso ,anche sospetto, o problema alla Dirigente e ai responsabili della sicurezza online;
- usare comportamenti sicuri, responsabili e professionali nel l'uso della tecnologia;
- garantire che le comunicazioni digitali con gli studenti dovrebbero essere a livello professionale e solo attraverso i sistemi scolastici, non attraverso meccanismi personali, per esempio -mail, telefoni cellulari, ecc.

I Docenti

Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti:

- aver letto, compreso e sottoscritto la presente policy
- 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 ,quindi non private;
- evitare partecipazione a gruppi di condivisione di whatsapp o altro, inerenti la scuola (gruppi classe, gruppi genitori, etc..), se non autorizzati dalla Dirigente;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- segnalare al Dirigente scolastico , al collaboratore del Dirigente scolastico e al referente sul bullismo, qualsiasi abuso, anche solo sospetto, rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dai protocolli qui adottati;
- Gli insegnanti sono responsabili delle TIC nell'ambito dell'attività didattica e hanno il compito di responsabilizzare gli alunni per divenire consapevoli dell'importanza della salvaguardia di un bene comune, seguendo le corrette norme di utilizzo;
- controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- comunicare al referente sul bullismo e alla Dirigente scolastica, 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;

- garantire la presenza di un docente o di un adulto responsabile durante l'utilizzo di Internet, della piattaforma o di altre TIC, da parte dei ragazzi;
- porre attenzione all'utilizzo di penne USB, CD/DVD o altri dispositivi esterni personali e dell'istituto;
- dare chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforma studenti ecc.), condividendo con gli alunni la netiquette e indicandone le regole;
- non divulgare le credenziali di accesso agli account (username e password) e/o, nel caso ne sia a conoscenza, alla rete wifi;
- non allontanarsi dalla postazione lasciandola incustodita, se non prima di aver effettuato la disconnessione;
- non salvare sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili;
- proporre agli alunni attività di ricerca di informazioni in rete fornendo opportunamente loro indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento.
- illustrare ai propri alunni le regole di utilizzo contenute nel presente documento;
- aver letto, compreso e sottoscritto la presente policy

Gli alunni

- 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.
- leggere, comprendere, ed accettare la esafety policy
- capire l'importanza di segnalare abusi, o l'uso improprio o l'accesso a materiali inappropriati;
- sapere quali azioni intraprendere se loro o qualcuno che conoscono si sente preoccupato o vulnerabile quando si utilizza la tecnologia on-line;
- conoscere e capire la politica relativa all'uso dei telefoni cellulari, fotocamere digitali dispositivi portatili;
- conoscere e capire la politica della scuola sull' uso di immagini e il cyberbullismo;
- capire l'importanza di adottare buone pratiche di sicurezza on-line quando si usano le tecnologie digitali fuori dalla scuola;
- assumersi la responsabilità di conoscere i benefici e i rischi di utilizzo di Internet e di altre tecnologie in modo sicuro, sia a scuola che a casa.
- non utilizzare propri dispositivi esterni personali senza aver acquisito il permesso da parte dell'insegnante;
- chiudere correttamente la propria sessione di lavoro.
- utilizzare le TIC ,SOLO ,su indicazioni del docente;
- accedere all'ambiente di lavoro con il corretto account (per gli alunni delle classi per le quali

è stato attivato un account google apps for education), non divulgandone le credenziali di accesso (username, password), e archiviare i propri documenti in maniera ordinata e facilmente rintracciabile nella cartella di ogni lim riferiti alla classe in cui è presente;

- non manomettere le impostazioni dei PC della scuola;

I genitori

- Sostenere e condividere 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 del computer e tenere sotto controllo l'uso che i figli fanno di internet e del telefonino in generale;
- Sostenere la scuola nel promuovere la sicurezza online e approvare la e-policy;
- Utilizzare gruppi di condivisione su whatsapp all'interno delle classi per comunicazioni inerenti la scuola , utilizzando un linguaggio appropriato e nel rispetto di tutti.

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.

Successivamente si condividerà nelle seguente modalità e a seconda degli attori interessati per raggiungere in modo più incisivo le singole parti:

La condivisione e comunicazione della politica di e-safety agli alunni:

- Attraverso la discussione in classe della policy nei primi giorni di scuola, con particolare riguardo al protocollo di utilizzo di internet per le nuove classi prime;
- Attraverso l'inserimento di un estratto di questo documento nel diario scolastico e in particolare dei comportamenti da attuare in caso di bisogno;
- Istruendo ed informando gli alunni riguardo all'uso responsabile e sicuro di internet precedentemente all'accesso alla rete;
- Dando comunicazione dell'elenco delle regole per la sicurezza on-line che sarà pubblicato in tutte le aule o laboratori con accesso a internet;
- Ponendo particolare attenzione nell'educazione sulla sicurezza relativamente agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili.
- La scuola promuoverà eventi e/o dibattiti informativi e formativi, in momenti diversi dell'anno, rivolti a tutto il personale, agli alunni e ai loro genitori, con il coinvolgimento di

esperti, sui temi oggetto di codesto Documento;

- Tra le misure di prevenzione che la scuola metterà in atto ci saranno, inoltre, azioni finalizzate a promuovere una cultura dell'inclusione, del rispetto dell'altro e delle differenze così che l'utilizzo di Internet e dei cellulari oltre che collocarci all'interno di un sistema di relazioni, ci renda consapevoli di gestire con un certo grado di trasparenza i rapporti che si sviluppino in tale ambiente, giungendo a riconoscere e gestire le proprie emozioni. A tal proposito si manterrà l'attivazione di uno "Sportello di ascolto" rivolto a tutti gli alunni, articolato in colloqui individuali e/o collettivi, al fine di migliorare il benessere personale e scolastico mediante un'attività di supporto della sfera emotiva, relazionale e comportamentale. Si prevede al suo interno, anche uno spazio riservato ai docenti e genitori al fine di individuare strategie efficaci per affrontare problematiche tipiche dell'età adolescenziale.

La condivisione e comunicazione della 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 discussa negli organi collegiali (consigli di interclasse/intersezione, collegio dei docenti) 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 informazione/formazione on-line del personale docente nell'uso sicuro e responsabile di internet, sia professionalmente che personalmente, sarà fornita a tutto il personale, anche attraverso il sito web della scuola;
- Il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC sarà supervisionato dall'Animatore digitale, che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici;
- 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.
- un confronto collegiale, su base annuale, circa la necessità di apportare modifiche e miglioramenti alla policy vigente;
- elaborazione di protocolli condivisi di intervento.

La condivisione e comunicazione della la politica di e-safety ai genitori :

- L'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di internet sarà attirata nelle news o in altre aree 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;
- La scuola fornirà ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di internet anche a casa;
- I docenti di classe forniranno ai genitori indirizzi sul web relativi a risorse utili per lo studio e a siti idonei per gli alunni funzionalmente alle attività didattiche progettate;

- si provvederà all'organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare;
 - Allo scopo di condividere regole comuni per l'utilizzo sicuro di Internet sia a casa che a scuola, si invitano tutti i genitori a prestare la massima attenzione ai principi e alle regole contenute nel presente documento;
 - Si richiede che ogni genitore e/o tutore si impegni a farle rispettare ai propri figli anche in ambito domestico, primariamente assistendo i minori nel momento dell'utilizzo della rete e poi ponendo in atto tutti i sistemi di sicurezza che aiutino a diminuire il rischio di imbattersi in materiale indesiderato.
-

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.

Le infrazioni alla policy possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori a docenti/ATA, referente cybebullismo, vicario del Dirigente e al Dirigente scolastico stesso.

Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso.

Il Dirigente scolastico ha la facoltà di revocare l'accessibilità temporanea o permanente ai laboratori informatici e/o all'utilizzo di strumenti tecnologici (pc, tablet, notebook, ecc) a chi non si attiene alle regole stabilite.

La scuola prenderà tutte le precauzioni necessarie per garantire la sicurezza on-line. Tuttavia, a causa della scala internazionale collegata ai contenuti Internet, la disponibilità di tecnologie mobili e velocità di cambiamento, non è possibile garantire che il materiale non idoneo apparirà mai su un computer della scuola o dispositivo mobile.

Né la scuola né l'autorità locale possono accettare la responsabilità per il materiale accessibile, o le conseguenze di accesso a Internet.

Al personale e agli alunni saranno date informazioni sulle infrazioni in uso e le eventuali sanzioni contenute nel Regolamento di Istituto o nel presente documento. Nel caso in cui le infrazioni della policy violino norme previste dal Regolamento di Istituto si procede secondo quanto previsto dal Regolamento stesso; qualora le infrazioni riguardino l'opportunità di certi comportamenti o la convivenza civile, la scuola eroga delle sanzioni secondo il principio della sensibilizzazione e del risarcimento dell'eventuale danno provocato, in uno spirito di recupero e rieducazione.

Nelle sezioni successive al presente documento sono, inoltre, richiamate e specificate le infrazioni e relative sanzioni.

I provvedimenti includono:

- Qualsiasi rilevamento di sospetto abuso, offesa, procurato disagio ricevuto su internet, sia personale che di un compagno, sarà sempre riferito, da parte del personale scolastico, al Dirigente Scolastico, al collaboratore del Dirigente e al referente del bullismo che fungeranno da primo punto di contatto;
- Possibile ritiro del cellulare fino a fine giornata;
- Saranno informati e documentati i genitori o i tutori per condividere con loro le strategie più opportune;
- Denunce di bullismo online saranno trattate in conformità con la legge attuale;
- Reclami relativi alla protezione dei bambini saranno trattati in conformità alle procedure di protezione dell'infanzia;
- Successivamente, nei casi più gravi, saranno avviate le comunicazioni alle autorità competenti;
- Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. Infatti è bene ricordare a tutti che nel momento in cui un qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia.

Disciplina degli alunni

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, in modo persistente, 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;
- l'invio o la condivisione di immagini intime o troppo spinte;
- il collegamento a siti web, nell'orario scolastico, non autorizzati dai docenti.
- L'utilizzo, non autorizzato o comunicato ai docenti, dello smartphone in orario scolastico (utilizzando messaggia, video, audio o foto).

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 gravità del comportamento.

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.

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 ed 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, al Dirigente scolastico, all'Animatore digitale.

Il Dirigente scolastico 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 il Dirigente scolastico 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.

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:

- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai;
- una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio;
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo;
- la mancanza di adeguata conoscenza che la responsabilità dei contenuti dello smartphone dei minori è sempre ascrivibile ai genitori/tutori ;
- assoluto disinteresse sui contenuti dello smartphone dei propri figli;

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.

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.

Le regole relative all'accesso ad Internet vengono approvate dal Collegio dei Docenti e dal Consiglio di Istituto e pubblicate sul sito della scuola.

Gli alunni vengono informati del fatto che l'utilizzo di Internet è monitorato e vengono date loro istruzioni per un uso responsabile e sicuro. Il personale scolastico riceve una copia del Regolamento, che viene sottoscritta e osservata scrupolosamente.

Tutto il personale scolastico, pertanto, è coinvolto nel monitoraggio dell'utilizzo di Internet, nello sviluppo delle linee guida e nell'applicazione delle istruzioni sull'uso sicuro e responsabile di Internet.

Il monitoraggio dell'implementazione della policy e del suo eventuale aggiornamento sarà svolta ogni anno. Tale monitoraggio sarà curato dal Dirigente scolastico con la collaborazione dell'Animatore digitale, dal referente del cyberbullismo e dai docenti delle classi, tramite questionari e conversazioni. Sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di internet. Il monitoraggio sarà rivolto anche agli insegnanti, al fine di valutare l'impatto della policy e la necessità di eventuali miglioramenti. L'aggiornamento della policy sarà curato dal Dirigente scolastico, dal referente cyberbullismo e dagli Organi Collegiali, a seconda degli aspetti considerati.

La E-Safety Policy si inserisce all'interno di altre politiche scolastiche, quali la politica di protezione dei minori, la politica anti-bullismo, la politica del benessere degli alunni a scuola.

Come già ricordato, la E-Safety Policy sarà riesaminata annualmente o quando si verificano cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola e tutte le modifiche della Policy saranno discusse in dettaglio con tutti i membri del personale docente.

Nell'ambito del monitoraggio dell'implementazione della E-Safety Policy si terranno in considerazione i dati annuali sulla base dei seguenti dati: **Anno Scolastico, Numero di segnalazioni, Numero di Infrazioni e Numero di sanzioni disciplinari**

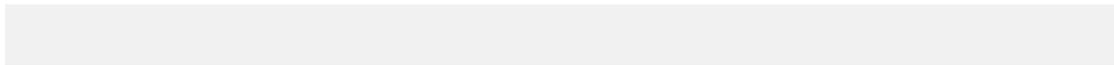
Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.

Azioni da svolgere nei prossimi 3 anni:

- 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



Capitolo 2 - Formazione e curriculum

2.1. Curriculum 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 curriculum digitale.

Il nostro Istituto condivide le linee indicate nel Piano Nazionale Scuola Digitale (PNSD) . Esse danno come indirizzo l'intento di modificare gli ambienti di apprendimento per rendere l'offerta formativa coerente con i cambiamenti della società della conoscenza e con le esigenze e gli stili cognitivi delle nuove generazioni.

Si ricorda il D.M. 851 del 27 ottobre 2015, in attuazione dell'art.1, comma 56 della legge 107/2015, che ne prevede l'attuazione al fine di:

- migliorare le competenze digitali degli studenti anche attraverso un uso consapevole delle stesse;
- implementare le dotazioni tecnologiche della scuola al fine di migliorare gli strumenti didattici e laboratoriali ivi presenti;
- favorire la formazione dei docenti sull'uso delle nuove tecnologie ai fini dell'innovazione didattica;
- individuare un Animatore Digitale ed un team per l'innovazione digitale che supporti ed accompagni adeguatamente l'innovazione didattica, nonché l'attività dell'animatore Digitale;

- partecipare a bandi nazionali ed europei per finanziare le suddette iniziative;

Curricolo sulle competenze digitali per gli studenti

Le Nuove Indicazioni Nazionali del 2012, in raccordo con il programma europeo Competenze chiave, prevedono che al termine del primo ciclo di istruzione lo studente possieda buone competenze digitali e sappia usare con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo. In questo senso le TIC (Tecnologie dell'Informazione e della Comunicazione) preparano gli studenti ad un'attiva e consapevole partecipazione ad un mondo in rapida evoluzione e nel quale è necessario acquisire abilità e competenze in grado di facilitare l'adattamento dell'individuo ai continui cambiamenti. Si rende quindi necessario lo sviluppo e la diffusione di una mentalità tecnologica diffusa e precoce, intesa come alfabetizzazione al senso, all'utilizzabilità in contesti dati e per scopi definiti da un lato ed acquisizione sempre più consapevole di strategie efficaci per il dominio di una macchina complessa che impiega e genera oggetti immateriali, dall'altro. Gli alunni dovrebbero quindi imparare ad utilizzare le TIC per cercare, esplorare, scambiare e presentare informazioni in modo responsabile, creativo e con senso critico, essere in grado di avere un rapido accesso a idee ed esperienze provenienti da persone, comunità e culture diverse. Alla scuola spetta quindi anche il compito di trovare raccordi efficaci tra la crescente dimestichezza degli alunni con le Tecnologie dell'Informazione e della Comunicazione e l'azione didattica quotidiana. Le TIC possono infatti offrire significative occasioni per sviluppare le competenze di comunicazione, collaborazione e problem-solving.

Nell'ambito del PNSD questa scuola si propone un programma di progressiva educazione alla sicurezza, online come parte del curriculum scolastico. Si impegna a sviluppare una serie di competenze e comportamenti adeguati alle età degli alunni e ad esperienza, tra cui:

- programmare attività e far partecipare gli alunni a laboratori di utilizzo consapevole e appropriato delle Tic;
- capire il comportamento accettabile quando si utilizza un ambiente online, vale a dire, essere educato, non utilizzare comportamenti inappropriati, mantenere le informazioni personali private;
- conoscere le conseguenze disciplinari della scuola, civili e penali in caso di denuncia e riscontro oggettivo di infrazioni inerente un utilizzo scorretto degli smartphone e contrario alla presente policy o al regolamento di istituto;
- capire il motivo per cui non devono pubblicare foto o video di altri senza il loro permesso;
- capire il motivo per cui qualsiasi materiale scritto, pubblicato e postato sui social è sempre tracciabile e può rimanere per sempre;
- capire che condividere è essere ugualmente responsabili di ciò che vi è all'interno del gruppo;
- capire perché 'amici' on-line potrebbero non essere chi dicono di essere e di comprendere perché dovrebbero fare attenzione in un ambiente online;
- sapere come restringere o affinare una ricerca;
- essere a conoscenza che l'autore di un sito web / pagina può avere un particolare pregiudizio;

- sviluppare una serie di strategie per valutare e verificare le informazioni prima di accettarne l'esattezza;
- utilizzare con attenzione Internet per garantire che si adatti alla loro età e supporti gli obiettivi di apprendimento per le aree curriculari specifiche;
- sapere come segnalare eventuali abusi tra cui il bullismo on-line e come a chiedere aiuto ai docenti, ai genitori, se si verificano problemi quando si utilizzano le tecnologie Internet;
- comprendere l'impatto di bullismo online, sexting, grooming e sapere come cercare aiuto se sono in pericolo;
- capire il motivo per cui non dovrebbero inviare o condividere resoconti dettagliati delle loro vite personali e informazioni di contatto;

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.

La formazione del corpo docente verrà organizzata su due livelli: interno ed esterno. A livello interno, nel PTOF, si prevede che una parte della formazione in servizio sia dedicata proprio all'uso e all'inserimento delle TIC nella didattica e ai temi informatici in generale. Tale formazione è svolta o da docenti dell'Istituto con formazione specifica o organizzando conferenze tenute da esperti esterni per permettere un' adeguata formazione agli insegnanti stessi.

Per quanto riguarda la formazione esterna, la scuola assicura tempestiva e capillare informazione su corsi, convegni e seminari che riguardino tali argomenti, cercando altresì di agevolare il personale che intenda parteciparvi. Infine la scuola può aderire a progetti appositi di formazione presentati da enti e associazioni, come già avvenuto in passato.

Sicuramente continueranno ad essere pianificate occasioni di formazione per apprendere l'utilizzo delle tecnologie e capirne le potenzialità e, probabilmente, saranno cercate risorse per dare seguito a quanto iniziato con i corsi di formazione sulle metodologie innovative e sull'integrazione delle TIC nella didattica.

La formazione dei docenti sull'utilizzo consapevole e sicuro di internet e delle tecnologie digitali

La formazione in ingresso e in servizio è senza dubbio il cardine per assicurare l'adeguatezza della professionalità docente ai bisogni formativi ed educativi degli studenti.

Prioritario, infatti, appare il coinvolgimento degli insegnanti ai quali vanno rivolti moduli di formazione che rafforzino le competenze necessarie a individuare tempestivamente eventuali risvolti psicologici conseguenti all'uso distorto delle nuove tecnologie e alla violenza in contesti faccia a faccia.

La scuola partecipa dal 2017/18 al programma "generazioni connesse" sul cui sito è disponibile una piattaforma di formazione destinata a tutti i docenti dell'Istituto che vogliano formarsi sull'argomento specifico delle nuove tecnologie.

Nel corso dell'a.s. 2017/18 sono stati organizzati due eventi : un momento di formazione ed informazione rivolto agli alunni sul tema del Bullismo e Cyberbullismo che ha visto la partecipazione di esponenti della Polizia di Stato, della Polizia Postale , di uno psicologo esperto in problematiche minorili e di Teresa Manes, autrice di un libro "Andrea dai panatoni rosa". Un altro evento è stato dedicato alle famiglie ed ai docenti. Si è trattato di un convegno dal titolo: **Insieme...per un bullo in meno . Il ruolo della scuola nella prevenzione e nel contrasto al cyberbullismo.** L'evento ha visto la partecipazione di figure professionali di alto rilievo: Il Presidente del Tribunale di Napoli Nord, il Sindaco della nostra città, dirigenti della Polizia di Stato e della Polizia Postale, Dirigente Scolastico e Referente bullismo e cyberbullismo della scuola.

Nel corso dell'a.s. 2019/20, nell'ambito delle iniziative della Regione Campania, si è svolto un seminario dal titolo **@scuolasenzabulli** per la prevenzione ed il contrasto al bullismo e cyberbullismo promosso dal Comitato Regionale per le comunicazioni della Campania. Al convegno hanno partecipato il Sindaco della nostra città , Presidente e Dirigente CORECOM Campania, Funzionari AGCOM, Dirigenti della Polizia Postale , Dirigente Scolastico e Referente bullismo e cyberbullismo della scuola.

Viste le positive reazioni di studenti, docenti e genitori e la necessità di implementare la **eSafety Policy** con il contributo di tutte le componenti, la Scuola continuerà ad organizzare per l'anno prossimo occasioni di confronto sulle strategie più opportune da adottare come promozione dell'utilizzo consapevole e sicuro di Internet e delle TIC e come misure di prevenzione primaria al (cyber)bullismo.

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

tecnologie digitali

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

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

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

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020)

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

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

- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza

digitale.

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

personali.

Il 25 maggio 2018 è entrato in vigore in tutti gli stati aderenti all'Unione Europea il Regolamento del Parlamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, conosciuto come GDPR.

Anche se in parte quanto previsto dal nuovo Regolamento risulta facilmente sovrapponibile alla precedente normativa italiana, è però necessario ricordare che il GDPR diventa il nuovo riferimento per garantire la corretta tutela dei dati personali. Pertanto il nostro Istituto si è adeguato alle modalità e responsabilità prescritte da questo documento .

L'Istituto Comprensivo "D. Cimarosa IV Circolo" di Aversa rispetta la privacy dei propri utenti e si impegna a proteggere i dati personali che gli stessi conferiscono all'I.C. stesso. La raccolta ed il trattamento di dati personali avvengono, quando necessari, in relazione all'esecuzione di servizi richiesti dall'utente, o quando l'utente stesso decide di comunicare i propri dati personali; in tali circostanze, la presente politica della privacy illustra le modalità ed i caratteri di raccolta e trattamento dei dati personali dell'utente. L'I.C. "D. Cimarosa IV Circolo " tratta i dati personali forniti dagli utenti in conformità alla normativa vigente. In caso di raccolta di dati personali, l'I.C. "D. Cimarosa IV Circolo " informerà l'utente sulle finalità della raccolta al momento della stessa, ove necessario, richiederà il consenso dell'utente. L'Istituto non comunicherà i dati personali dell'utente a terzi senza il consenso dello stesso. Se l'utente decide di fornire alla scuola i propri dati personali, la scuola potrà comunicarli all'interno dell'Istituto od a terzi che prestano servizi alla scuola, solo rispetto a coloro che hanno bisogno di conoscerli in ragione delle proprie mansioni, e, ove necessario, con il permesso dell'utente. La scuola tratta i dati personali dell'utente per le seguenti finalità di carattere generale: per soddisfare le richieste a specifici prodotti o servizi, per personalizzare la visita dell'utente al sito, per aggiornare l'utente sulle ultime novità in relazione ai servizi offerti od altre informazioni che ritiene siano di interesse dell'utente che provengono direttamente dall'Istituto o dai suoi partners, e per comprendere meglio i bisogni dell'utente ed offrire allo stesso servizi migliori. Il trattamento di dati personali dell'utente da parte dell'Istituto per le finalità sopra specificate avviene in conformità alla normativa vigente a tutela dei dati personali.

Infine, si fa riferimento a tutto quanto previsto dal Decreto legislativo 30 giugno 2003, n. 196 (c. d. Codice della Privacy). Tuttavia, si possono individuare al riguardo alcune linee guida di e- safety:

- Non violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici. Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale e non alla diffusione. Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini su Internet, e sui social network in particolare. (da vademecum privacy del Garante);
- In caso di comunicazione sistematica o diffusione diventa infatti necessario, di regola, ottenere il consenso informato delle persone presenti nelle fotografie e nei video. Si deve quindi prestare particolare attenzione prima di caricare immagini e video su blog o social network, oppure di diffonderle attraverso mms o sistemi di messaggistica istantanea. Succede spesso, tra l'altro, che una fotografia inviata a un amico o a un familiare venga poi

inoltrata ad altri destinatari, generando involontariamente una comunicazione a catena dei dati personali raccolti. Tale pratica può dar luogo a gravi violazioni del diritto alla riservatezza delle persone riprese, e fare incorrere in sanzioni disciplinari, pecuniarie e in eventuali reati. (da vademecum privacy del Garante);

- L'utilizzo di telefoni cellulari, di apparecchi per la registrazione di suoni e immagini, quando autorizzato dai docenti, è consentito, ma esclusivamente per fini personali, e sempre nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte (siano essi studenti o professori) in particolare della loro immagine e dignità.

Le istituzioni scolastiche hanno, comunque, la possibilità di regolare o di inibire l'utilizzo di registratori, smartphone, tablet e altri dispositivi elettronici all'interno delle aule o nelle scuole stesse. Gli studenti e gli altri membri della comunità scolastica, in ogni caso, non possono diffondere o comunicare sistematicamente i dati di altre persone (ad esempio pubblicandoli su Internet) senza averle prima informate adeguatamente e averne ottenuto l'esplicito consenso. (da vademecum privacy del Garante)

Registrazione delle lezioni e strumenti compensativi

È possibile registrare la lezione esclusivamente per scopi personali, ad esempio per motivi di studio individuale. Per ogni altro utilizzo o eventuale diffusione, anche su Internet, è necessario prima informare adeguatamente le persone coinvolte nella registrazione (professori, studenti...) e ottenere il loro esplicito consenso. Nell'ambito dell'autonomia scolastica, gli istituti possono decidere di regolamentare diversamente o anche di inibire l'utilizzo di apparecchi in grado di registrare. In ogni caso deve essere sempre garantito il diritto degli studenti con diagnosi DSA (disturbi specifici dell'apprendimento) o altre specifiche patologie di utilizzare tutti gli strumenti compensativi (come il registratore) di volta in volta previsti nei piani didattici personalizzati che li riguardano. (da vademecum privacy del Garante).

- È consigliabile utilizzare canali istituzionali per comunicazioni a scopo didattico con le famiglie e gli studenti
- Come e-mail si utilizzerà quella istituzionale della scuola (@cimarosaaversa.edu.it) per averne tracciabilità della conversazione in un luogo protetto.
- Le fotografie o i video da pubblicare sul sito che includano allieve e allievi saranno selezionati con cura e non permetteranno a singoli di essere chiaramente identificati a meno che non si tratti di eventi particolari per cui le famiglie potranno concedere opportuna autorizzazione. La scuola cercherà di utilizzare fotografie o video di gruppo piuttosto che foto integrali di singoli.
- I nomi completi di alunne e alunni saranno evitati sul sito web come pure nei blog, forum e wiki, in particolare se in associazione con le loro fotografie.
- All'atto dell'iscrizione è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico di immagini e video delle/dei minori secondo i principi sopra indicati.
- Ogni caso particolare sarà preso in considerazione per stabilire l'opportunità di pubblicare dati personali e sarà presentata apposita richiesta circostanziata che varrà solo per lo specifico evento.

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.

La scuola metterà in atto tutte le azioni necessarie per garantire agli studenti l'accesso alla documentazione cercata adottando tutti i sistemi di sicurezza conosciuti per diminuire le possibilità di rischio durante la navigazione.

Resta fermo che non è possibile garantire una navigazione totalmente priva di rischi e che la Scuola

e gli insegnanti non possono assumersi le responsabilità conseguenti all'accesso accidentale e/o improprio a siti illeciti.

Accesso a internet (filtri, antivirus, navigazione)

Il nostro Istituto ha configurato un proxy server per monitorare il traffico web e per bloccare l'accesso a siti inappropriati a un contesto scolastico.

Occorre, inoltre, sensibilizzare tutta la comunità scolastica sull'opportunità di mantenere aggiornati gli antivirus installati sulle macchine personali e controllare i dispositivi di archiviazione esterna che vengano collegati al proprio pc.

Le principali norme sono:

- L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante;
- Internet non può essere usato per scopi vietati dalla legislazione vigente;
- L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet;
- E' vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza.
- Consultare obbligatoriamente prima di installare qualsiasi programma l'animatore digitale, un responsabile di laboratorio o un tecnico per valutarne la compatibilità

Linee guida di buona condotta dell'utente e buone pratiche nell'uso della rete

- Rispettare la legislazione vigente;
- Tutelare la propria privacy, quella degli altri utenti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui hai accesso;
- Rispettare la cosiddetta netiquette (regole condivise che disciplinano il rapportarsi fra utenti della rete, siti, forum, mail e di qualsiasi altro tipo di comunicazione).
- Controllo della validità e dell'origine delle informazioni a cui si accede o che si ricevono;
- Utilizzo di fonti alternative di informazione per proposte comparate;
- Ricerca del nome dell'autore, dell'ultimo aggiornamento del materiale e di altri possibili link al sito;
- Rispetto dei diritti di autore e dei diritti di proprietà intellettuale.

Gestione accessi (Password, backup, etc..)

Accesso docenti

L'Istituto attualmente è dotato di una rete wireless destinata all' utilizzo didattico da parte del corpo docente. La password è unica a livello di Istituto/plesso. Ai docenti è consentito accedere ad Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto previa richiesta alla Dirigente il quale ne darà l'autorizzazione.

I computer portatile presenti nelle aule non richiedono una password di accesso per

l'accensione. Ogni docente è quindi tenuto ad un controllo della strumentazione in aula poiché l'uso del dispositivo è permesso agli alunni solo su autorizzazione dell'insegnante. Ogni docente accede al registro elettronico attraverso una password che non può essere comunicata a terzi, né agli alunni.

Accesso studenti

Il Regolamento di Istituto vieta l'uso del cellulare. In particolare, agli studenti non è consentito accedere ad Internet da propri dispositivi utilizzando la rete Wi-Fi dell'Istituto. Durante l'orario scolastico agli alunni non è permesso l'utilizzo della telefonia mobile; è altresì vietato l'uso per scopo personale di tutti gli altri strumenti informatici di proprietà e non dello studente. L'eventuale utilizzo di strumenti informatici di proprietà dello studente durante l'attività didattica deve essere autorizzata dal docente. Relativamente agli alunni che accedono a Internet durante l'attività didattica sono consentiti la navigazione guidata da parte dell'insegnante e la stesura di documenti collaborativi purché sotto il controllo dell'insegnante e nel caso in cui tale attività faccia parte di un progetto di lavoro precedentemente autorizzato. E' vietato l'accesso alle chat-room pubbliche o non moderate. La trasgressione a queste regole avranno sanzione decisa dal Dirigente e dal CdC secondo le presenti norme e in accordo al Regolamento di Istituto.

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.

Gli studenti non possono utilizzare i propri dispositivi durante le attività didattiche come previsto dal regolamento di istituto, né possono accedere alla rete attraverso i dispositivi della scuola se non con autorizzazione dell'insegnante presente in aula e comunque per ricerche attinenti le attività didattiche. Individui con disturbi specifici di apprendimento o altre disabilità certificate, previa consultazione con il Consiglio di Classe, concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili e le modalità di custodia degli stessi.

Nel caso in cui debbano comunicare con la famiglia durante l'orario scolastico, alunne e alunni possono usare gratuitamente la linea fissa della scuola rivolgendosi ad un collaboratore scolastico ; allo stesso modo le famiglie devono chiamare il centralino della scuola se hanno assoluta necessità di comunicare qualcosa ai propri figli. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.

L'invio di materiali abusivi, offensivi o inappropriati è vietato, anche se avviene all'interno di cerchie

o gruppi di discussione privati.

Avuto inoltre riguardo per il fatto che gli smartphone possono essere utilizzati anche per scattare foto (o effettuare riprese filmate) e per trasferirle con un MMS chissà a chi e chissà dove, 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.

In particolare , a riguardo di un uso scorretto dello smartphone, si ricorda che:

- 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 (magari solo per curiosità) chissà quando e chissà dove.
- 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.
- 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 fa uso di un device (smartphone o tablet) durante l'orario scolastico e lo utilizza in modo scorretto e contro il regolamento di istituto 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.

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.

Nella scuola primaria si chiede alle famiglie di non lasciare tali dispositivi ad alunne e alunni. Nella scuola secondaria, i telefoni cellulari vanno spenti prima dell'ingresso a scuola e riaccesi una volta lasciato l'istituto. Una volta entrati in classe gli alunni riporranno il proprio dispositivo nell'apposito contenitore dell'aula e lo riprenderanno a fine giornata scolastica. Se - malgrado il divieto appena espresso - gli studenti verranno sorpresi ad usare il cellulare, verrà chiesto al docente di prenderlo in custodia temporaneamente e consegnarlo in Presidenza e/o dal DSGA. Il dispositivo verrà chiuso a chiave fino al termine delle lezioni e poi restituito alla famiglia convocata o, in mancanza di questa, al ragazzo stesso. Verrà immediatamente comunicato l'accaduto al Dirigente e al suo primo collaboratore. Si convocheranno per vie brevi i genitori interessati ai quali verrà, possibilmente, riconsegnato il cellulare.

Per la componente personale scolastico docenti/ata

I docenti possono utilizzare i dispositivi della scuola per realizzare tutte le attività connesse alla funzione docente. E' consentito per i docenti l'uso dei propri dispositivi in classe per quanto attiene l'attività didattica qualora siano necessari, ma non possono essere utilizzati durante le lezioni per questioni personali.

Il personale preferirà, quando ciò è possibile, l'impiego della strumentazione fornita dalla scuola rispetto a quella personale (portatili, pc fissi, ...); le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali. Telefoni cellulari, tablet, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante le lezioni scolastiche se non all'interno di attività didattiche programmate. L'uso improprio della rete è contestato al titolare delle credenziali con cui è avvenuta la comunicazione. Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (chiavette usb, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.

Durante l'attività didattica è opportuno che ogni insegnante: - dia chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforma studenti ecc.), condividendo con gli studenti la netiquette e indicandone le regole; - si assuma la responsabilità di segnalare prontamente eventuali malfunzionamenti o danneggiamenti al tecnico informatico; - non salvi sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili e proponga agli alunni attività di ricerca di informazioni in rete fornendo opportunamente loro indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola

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

- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto 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.

Il nostro istituto integra l'offerta formativa con attività finalizzate alla prevenzione e al contrasto del bullismo e del cyberbullismo, nell'ambito delle tematiche afferenti a Cittadinanza e Costituzione per tradurre i "saperi" in comportamenti consapevoli e corretti, indispensabili a consentire alle giovani generazioni di esercitare la democrazia nel rispetto della diversità e delle regole della convivenza civile. Le indicazioni relative ad un utilizzo sicuro della Rete da parte degli studenti potranno essere oggetto di specifici moduli didattici, da inserire nel Piano dell'Offerta Formativa (POF).

La strategia di contrasto dei fenomeni del bullismo dovrebbe essere costituita, quindi, già a partire dalle scuole primarie, da un insieme di misure di prevenzione rivolte agli studenti di varia tipologia.

Di seguito una tabella dei possibili rischi online ed i suggerimenti per azioni specifiche.

RISCHI	AZIONI
Adescamento online (grooming)	Sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione. Qualora si venga a conoscenza di casi simili, occorre valutarne la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.
Cyberbullismo	Campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni. I casi possono essere molto variegati, variando dal semplice scherzo di cattivo gusto via sms/Whatsapp a vere e proprie minacce verbali e fisiche, che costituiscono reato. Occorre confrontarsi con il Dirigente Scolastico sulle azioni da intraprendere.
Dipendenza da Internet, videogiochi, shopping o gambling online, ...	Informazioni sul fatto che ciò può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito a insaputa di altri) rappresenta un vero e proprio illecito.
Esposizione a contenuti pornografici, violenti, razzisti, ...	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione e sensibilizzazione sulla necessità di monitorare l'esperienza online dei propri figli. Verso la componente studentesca: inserimento nel curriculum di temi legati alla affidabilità delle fonti online, all'interculturalità e al rispetto delle diversità. Qualora si venga a conoscenza di casi simili, occorre convocare i genitori per richiamarli a un maggiore controllo sulla fruizione di Internet da parte dei propri figli e/o sulla necessità di non usufruirne in presenza degli stessi.
Sexting e pedopornografia	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione. Verso la componente studentesca: inserimento nel curriculum di temi legati all'affettività, alla sessualità e alle differenze di genere. In casi simili, se l'entità è lieve occorre in primo luogo parlarne con alunne e alunni e rispettivi genitori, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. Chi è immerso dalla nascita nelle nuove tecnologie spesso non è consapevole che una foto o un video diffusi in rete potrebbero non essere tolti mai più né è consapevole di scambiare o diffondere materiale pedopornografico. In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico per gli adempimenti del caso.
Violazione della privacy	Informazione sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farle rispettare. Se il comportamento rilevato viola solo le norme di buona convivenza civile e di opportunità, occorre convocare i soggetti interessati per informarli e discutere dell'accaduto e concordare forme costruttive ed educative di riparazione. Qualora il comportamento rappresenti un vero e proprio illecito, il Dirigente Scolastico deve esserne informato in quanto a seconda dell'illecito sono previste sanzioni amministrative o penali.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

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

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

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

Il nostro Istituto si preoccuperà di attivare iniziative di informazione e formazione specifica attraverso uno o più incontri con gli studenti personale scolastico tutto e famiglie per la prevenzione ed il contrasto al cyberbullismo.

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 si preoccuperà di attivare iniziative di informazione specifica attraverso uno o più incontri informativi per la prevenzione dell'hate speech e rispetto degli altri.

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?

Il nostro Istituto si preoccuperà di attivare iniziative di informazione specifica attraverso uno o più incontri informativi per la prevenzione della dipendenza da internet e gioco online.

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 medialmente 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 si preoccuperà di attivare iniziative di informazione specifica attraverso uno o più incontri informativi per la prevenzione del rischio di sexting e per la tutela della propria privacy.

4.6 - Adescamento online

Il **grooming** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenzialmente 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 si preoccuperà di attivare iniziative di informazione specifica attraverso uno o più incontri informativi relativi al reato di adescamento online.

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 si preoccuperà di attivare iniziative di informazione specifica attraverso uno o più incontri informativi relativamente al reato di pedopornografia.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.

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

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- Promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale.

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/le studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online:** se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting:** nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

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

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di [Helpline 19696](#) e [Chat di Telefono Azzurro](#) per supporto ed emergenze;
- [Clicca e segnala di Telefono Azzurro](#) e [STOP-IT di Save the Children Italia](#) per segnalare la presenza di materiale pedopornografico online.

5.2. - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola 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](tel:19696).

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.

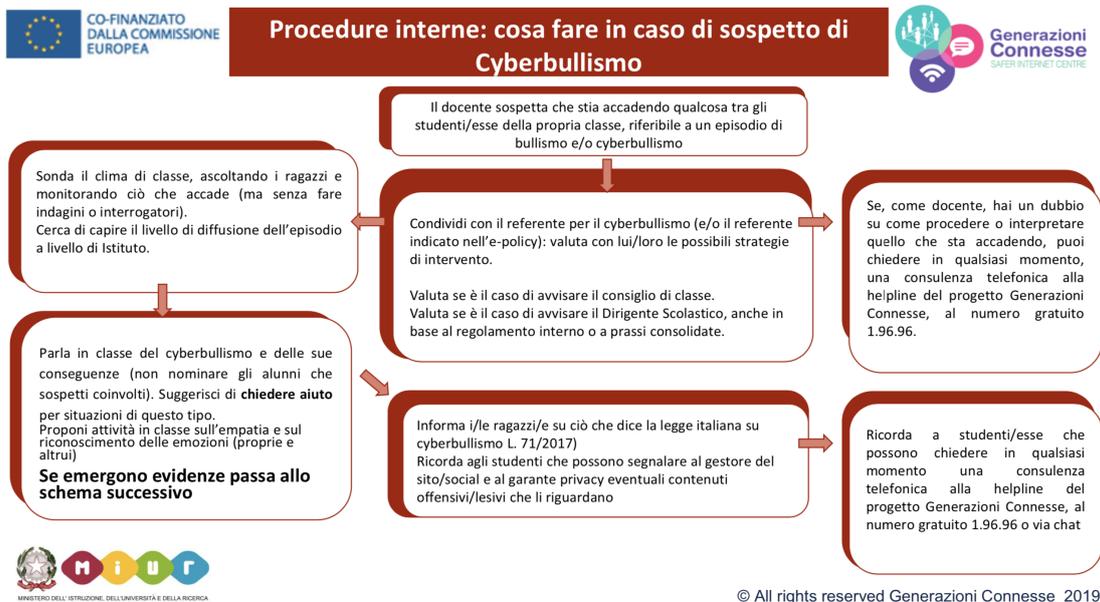
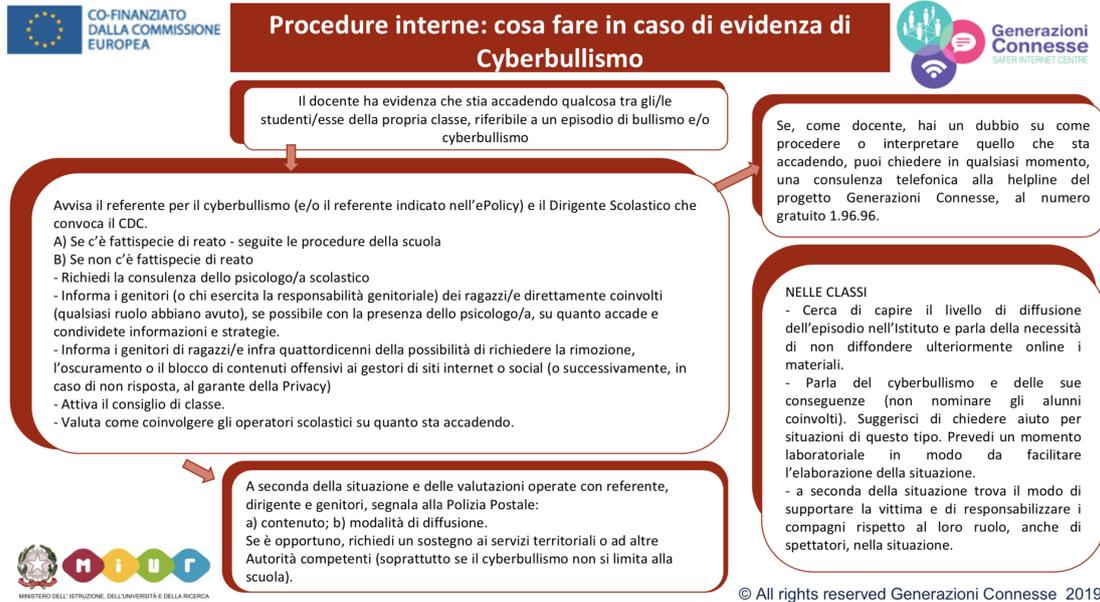
Per una mappatura degli indirizzi di tali strutture è possibile consultare il [Vademecum](#) di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza 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.

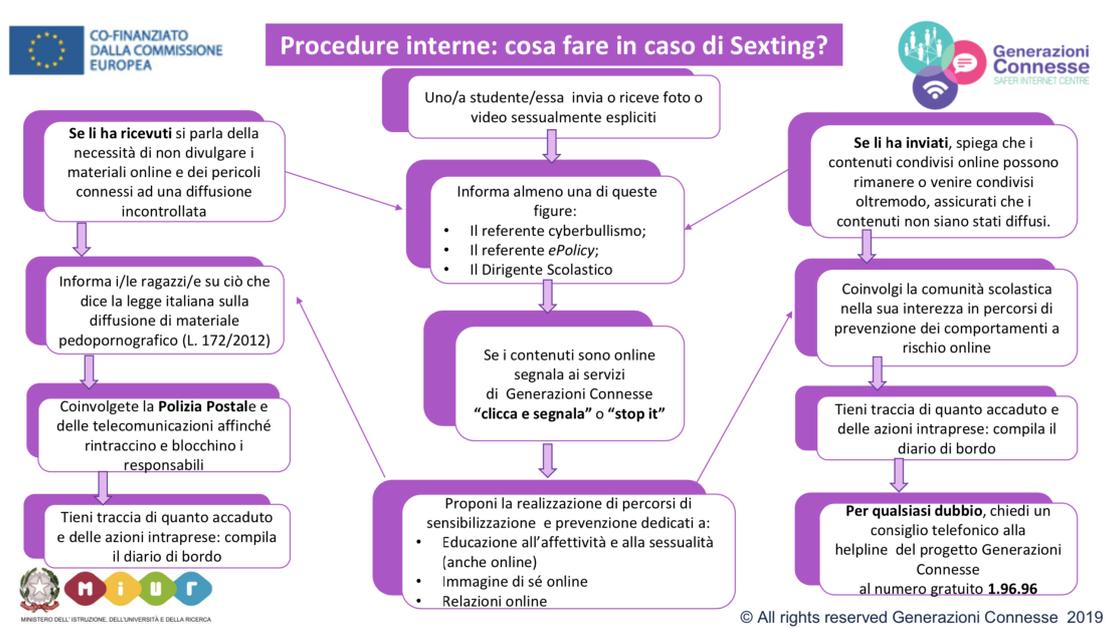
- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

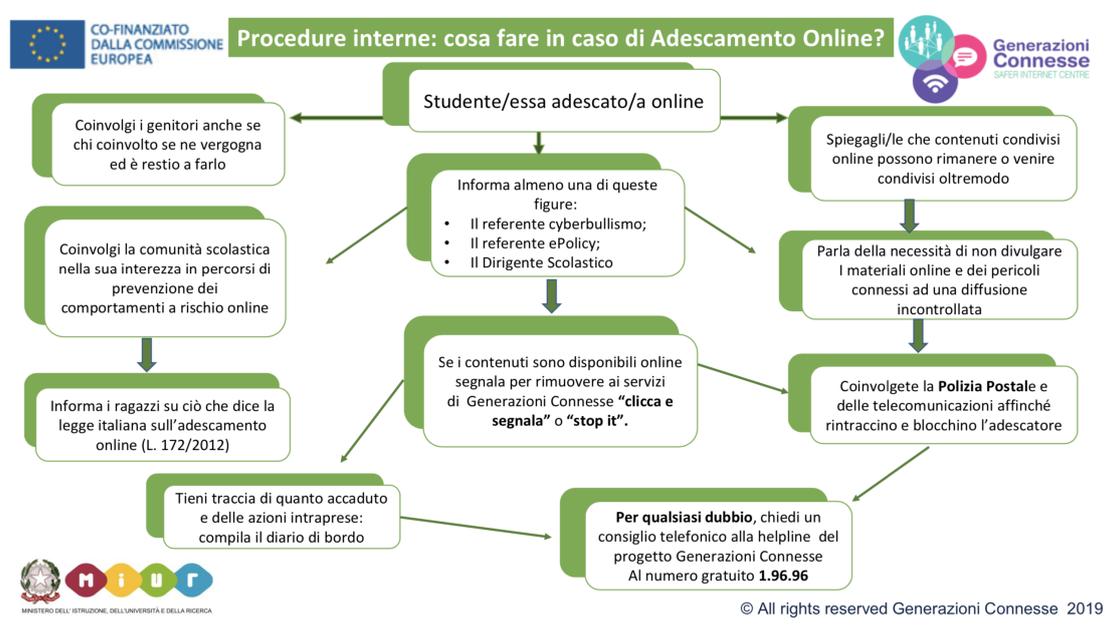
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



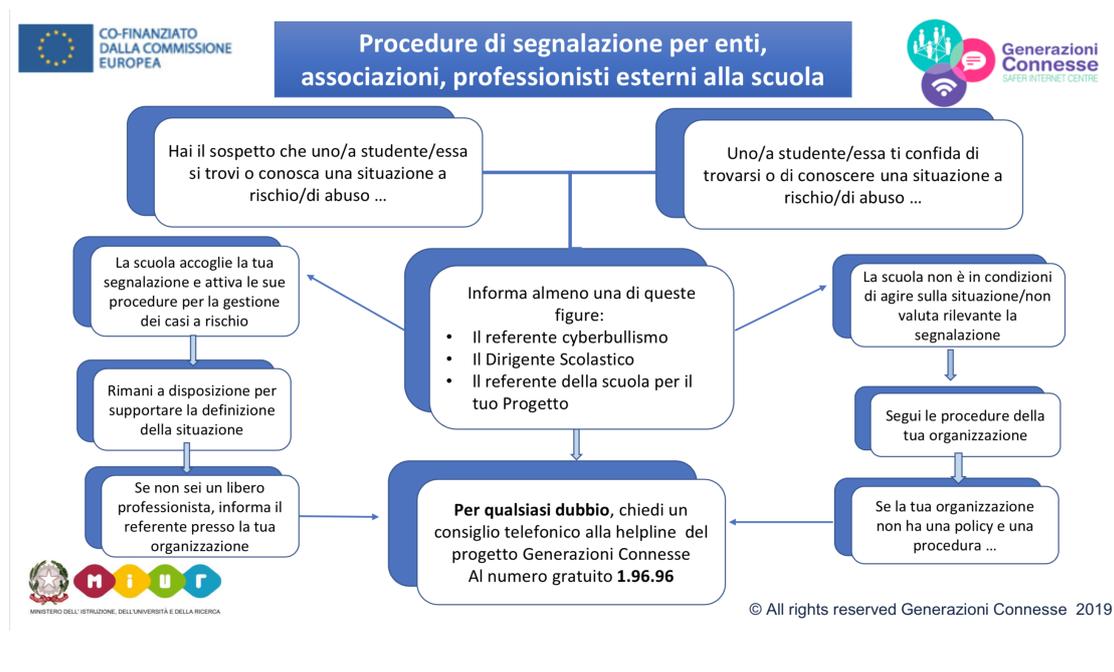
Procedure interne: cosa fare in caso di sexting?



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

