



ISTITUTO COMPRENSIVO "G. CALOPRESE" - SCALEA (CS)

Tel./Fax 0985 20988 – VIA F. DEGLI UBERTI, 1

www.icscalea.edu.it

E-Mail: csic8ay00b@istruzione.it - PEC: csic8ay00b@pec.istruzione.it

C.M. CSIC8AY00B - C.F. 82000990786

Documento di ePolicy



a.s. 2020/2021

CAP. 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 nell'apprendimento degli studenti e delle studentesse. Le ultime vicende relative al Covid-19 hanno dimostrato ed evidenziato, inoltre, il ruolo fondamentale di tali tecnologie in contesti didattici nuovi e anche emergenziali. Per tale motivo, diventa ancora più importante 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, dunque, 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.

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

La capacità di partecipare in modo costruttivo e consapevole alle comunità online e ai network virtuali costituisce un prerequisito fondamentale per essere parte attiva della società della conoscenza e dell'informazione. È fondamentale quindi sapere come ci si comporta in queste comunità, quali regole vanno rispettate e quali ruoli e responsabilità hanno i soggetti che vi partecipano. Di seguito il ruolo e le responsabilità delle figure coinvolte nella promozione dell'uso consapevole della rete.

▪ Il Dirigente Scolastico

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

- garantire la sicurezza, anche online, di tutti i membri della comunità scolastica;
- garantire una corretta formazione del personale scolastico sulle tematiche relative all'uso sicuro e consapevole di internet e della rete;
- promuovere la cultura della sicurezza online e garantisce una formazione adeguata del personale docente relativo all'uso delle TIC nella didattica;
- 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;

- gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali.

▪ **L'Animatore digitale**

Il ruolo dell'Animatore digitale include i seguenti compiti:

- supportare il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali;
- promuovere percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale";
- monitorare e rilevare eventuali episodi o problematiche connesse all'uso delle TIC a scuola;
- controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione);
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".

▪ **Il Referente bullismo e cyberbullismo**

Il Referente per il contrasto al bullismo e cyberbullismo ha il compito di¹:

- coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo, avvalendosi, inoltre, anche della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio che collaborano con l'Istituto (Associazione Gianfrancesco Serio, Punto Luce Scalea di Save the Children, Centro Donna Scalea, Associazione Banca del Tempo Scalea, Coop.soc. Progetto Germano, Movimento giovani SottoSopra Scalea, Coop. soc. EDI onlus, Associazione Civitas Solis...);
- coinvolgere con progetti e percorsi formativi *ad hoc* studenti, colleghi e genitori anche in collaborazione con le associazioni del territorio (Associazione Gianfrancesco Serio, Punto Luce Scalea di Save the Children, Comitato Genitori Connessi Scalea).

▪ **I Docenti**

i Docenti hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete e, pertanto hanno il compito di:

- 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;
- integrare il curriculum della propria disciplina con approfondimenti *ad hoc*, promuovendo l'uso delle tecnologie digitali nella didattica;
- garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;
- accompagnare e supportare gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete;
- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo all'Animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;

¹Per un approfondimento maggiore sui ruoli relativi alle problematiche del bullismo e del cyberbullismo (modulo 4, paragrafo 4.2.) cfr. *infra*.

- segnalare, sia per dovere morale che professionale, al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

▪ **Il personale Amministrativo, Tecnico e Ausiliario (ATA)**

Il personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il dirigente scolastico e con il personale docente tutto.

a) Il ruolo del **direttore dei servizi generali e amministrativi** include i seguenti compiti:

- 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.

Il **personale ATA**, inoltre, in relazione al regolamento di Istituto, è coinvolto nel compito di segnalare comportamenti non adeguati e/o episodi di bullismo/cyberbullismo e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi riconducibili ai suddetti episodi.

▪ **Gli Studenti e le Studentesse**

Gli Studenti e le Studentesse, in relazione al proprio grado di maturità e apprendimento, hanno il compito di:

- utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti;
- adottare condotte rispettose anche quando si comunica in rete;
- imparare a tutelarsi online attraverso il supporto della scuola e delle diverse figure;
- tutelare e rispettare i/le propri/e compagni/e;
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori;
- partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete e farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education (ad esempio, nel progetto S.C.A.T.T.I., gli/le alunni/e della secondaria si impegneranno, con il tutoraggio di un formatore esperto in TD e di uno psicologo, in un percorso mirato alla consapevolezza ed all'uso positivo delle TD; nella seconda parte del suddetto percorso loro stessi/e si faranno portatori/trici degli apprendimenti acquisiti, coinvolgendo l'intera platea studentesca attraverso azioni di peer education, utilizzando allo scopo proprio le TD, i social, tutorial, testimonianza in video, ecc.).

▪ **I Genitori**

I Genitori, in continuità con l'Istituto scolastico, dovranno:

- essere partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali;
- relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet;
- accettare e condividere quanto scritto nell'ePolicy dell'Istituto.

La scuola coglierà ogni occasione per sensibilizzare i genitori attraverso incontri con la Polizia municipale ed altri esperti o educatori, circolari, sito web e altre comunicazioni telematiche, informazioni su campagne di sicurezza promosse da altre istituzioni o su convegni dedicati a questo tema. I genitori saranno incoraggiati a sostenere la scuola nel promuovere le buone pratiche digitali e a seguire le linee guida sull'uso appropriato di immagini e video registrati in occasione di eventi scolastici – anche al di fuori delle aule – nonché accesso alle sezioni del sito dedicate ai genitori, con particolare riguardo al registro elettronico e agli ambienti virtuali istituzionali.

▪ **Gli Enti educativi esterni e le associazioni**

gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola dovranno:

- conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC;
- promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

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'E-POLICY ALL'INTERA COMUNITÀ SCOLASTICA

Il documento di E-policy verrà condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. Il documento, dopo l'approvazione da parte del Collegio dei Docenti e del Consiglio di Istituto, sarà esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque in vari punti spaziali dell'Istituto.

L'E-policy verrà condivisa e comunicata a tutta la 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 (a partire dall'a.s. 2021/2022);
- l'insegnamento trasversale di educazione civica².

Gli studenti e le studentesse verranno informati sul fatto che sono monitorati e supportati nella navigazione online, negli spazi della scuola e sulle regole di condotta da tenere in Rete, in modo da fornire loro norme condivise di sicurezza e prevenire comportamenti a rischio sia personali che dei/delle propri/e compagni/e. Ciascun attore scolastico (dai docenti agli/lle studenti/esse) si farà a sua volta promotore del documento in relazione al proprio ruolo.

I docenti, ai quali saranno riservati anche i corsi di Generazioni Connesse, potranno confrontarsi sui contenuti, sulle pratiche indicate e su come inserire nel curriculum le tematiche di interesse per poi elaborare miglioramenti alla policy vigente.

Per i genitori saranno organizzati incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare anche in collaborazione con gli enti del territorio. Grazie a due progetti di cui la nostra scuola è partner, questa azione sarà particolarmente potenziata: con il progetto Crescere in Calabria - nell'ambito della azione Fare Comunità - e con il progetto S.C.A.T.T.I., con una serie di incontri con formatori e psicologi/e, che accompagnano i genitori sia sul piano dell'educazione positiva sia sulle tecnologie digitali. Rientra in quest'ultimo percorso la nascita di un comitato, denominato GENITORI CONNESSI, che ha tra gli scopi quello di essere una rete di mutuo-aiuto tra genitori; una sorta di peer education genitoriale, che possa supportare chi è più in difficoltà con piattaforme e mondo digitale.

² Si rimanda al Ptof dell'Istituto.

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

1.5 - GESTIONE DELLE INFRAZIONI ALLA E-POLICY

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. Gli interventi previsti per gli alunni sono rapportati all'età e al livello di sviluppo dell'alunno. Più gli alunni sono piccoli, infatti, 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 provvedimenti disciplinari proporzionati all'età e alla gravità del comportamento.

a) SANZIONI DECISE DAL SINGOLO DOCENTE:

- il richiamo verbale;
- invito alla riflessione individuale;
- consegna da svolgere in classe significativa e commisurata;
- sospensione temporanea delle attività ludiche dell'intervallo;
- ammonizione scritta sul libretto personale o quaderno delle comunicazioni;
- ammonizione scritta sul registro di classe e riportata sul libretto personale o quaderno delle comunicazioni, eventualmente controfirmata dal Dirigente Scolastico.

b) SANZIONI DECISE DAL CONSIGLIO DI CLASSE SENTITO IL PARERE DEL DIRIGENTE SCOLASTICO:

- Ammonizione scritta ufficiale da parte del Dirigente Scolastico;
- Diffida scritta con comunicazione alla famiglia da parte del Dirigente Scolastico;
- Sospensione delle visite guidate, viaggi d'istruzione, gruppi sportivi o altre attività con l'obbligo della presenza a scuola con altre mansioni concordate;
- sospensione delle lezioni con o senza obbligo di frequenza fino a tre giorni;
- sospensione delle lezioni con o senza obbligo di frequenza fino a quindici giorni;
- sospensione oltre i quindici giorni solo nel caso di fatti di rilevanza penale o pericolo per l'incolumità delle persone tali da richiedere l'intervento degli Organi Istituzionali di Competenza³.

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.

Per quanto riguarda il **personale scolastico**, esso è tenuto ad un uso responsabile e adeguato delle TIC e dei servizi della scuola, rispettando la normativa vigente in relazione al trattamento dei dati personali, comuni e sensibili degli alunni, la segretezza delle password e la custodia degli strumenti e degli accessi di cui possono approfittare terzi. Tutto il personale è tenuto a collaborare con il Dirigente Scolastico e a fornire ogni informazione utile per le valutazioni di singoli casi in cui vi è il sospetto di una violazione delle norme indicare, nonché 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.

In considerazione dell'età dei discenti, le azioni e la condotta dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola e, pertanto, i genitori degli alunni possono essere convocati a scuola per concordare misure educative sanzionatorie anche a norma di legge.

1.6 - MONITORAGGIO DELL'IMPLEMENTAZIONE DELLA POLICY E SUO AGGIORNAMENTO

Il Regolamento dell'Istituto Scolastico verrà 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

³ Si rimanda al Patto di Corresponsabilità e al Regolamento di Istituto.

oggetto. Il monitoraggio dell'implementazione della policy sarà svolta ogni anno e sarà curato dal Dirigente scolastico con la collaborazione dell'Animatore digitale, del responsabile ePolicy e del referente Bullismo e Cyberbullismo, nonché 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.

1.7 - INTEGRAZIONE DELL'EPolicy CON REGOLAMENTI ESISTENTI

La policy si integrerà con il Regolamento di Istituto, Patto di Corresponsabilità e norme comportamentali relative all'uso delle dotazioni tecnologiche della Scuola, della rete wifi e del traffico internet e dei Laboratori informatici.

Azioni da svolgere entro un'annualità scolastica

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

Azioni da svolgere nei prossimi 3 anni

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

CAP. 2 - FORMAZIONE E CURRICOLO

2.1 - CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI

I ragazzi usano la Rete quotidianamente, talvolta in modo più intuitivo ed agile rispetto agli adulti, ma non per questo sono dotati di maggiori e consolidate 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. Il nostro Istituto, infatti, in relazione alla competenza digitale, prevede le seguenti conoscenze, abilità, nonché atteggiamenti:

Competenza digitale	
Conoscenze	Comprendere in che modo le tecnologie digitali possono essere di aiuto alla comunicazione, alla creatività e all’innovazione, pur nella consapevolezza di quanto ne consegue in termini di opportunità, limiti, effetti e rischi. Comprendere i principi generali, i meccanismi e la logica che sottendono alle tecnologie digitali in evoluzione. Conoscere il funzionamento e l’utilizzo di base di diversi dispositivi, software e reti. Assumere un approccio critico nei confronti della validità, dell’affidabilità e dell’impatto delle informazioni e dei dati resi disponibili con strumenti digitali. Essere consapevoli dei principi etici e legali chiamati in causa con l’utilizzo delle tecnologie digitali.
Abilità	Essere in grado di utilizzare le tecnologie digitali come ausilio per la cittadinanza attiva e l’inclusione sociale, la collaborazione con gli altri e la creatività nel raggiungimento di obiettivi personali, sociali o commerciali. Utilizzare, accedere a, filtrare, valutare, creare, programmare e condividere contenuti digitali. Essere in grado di gestire e proteggere informazioni, contenuti, dati e identità digitali. Riconoscere software, dispositivi, intelligenza artificiale o robot e interagire efficacemente con essi.
Atteggiamenti	Atteggiamento riflessivo e critico, ma anche improntato alla curiosità, aperto e interessato al futuro della loro evoluzione. Approccio etico, sicuro e responsabile all’utilizzo di tali strumenti.

L’uso consapevole e responsabile delle tecnologie digitali, in particolar modo in un contesto didattico nuovo con DAD e DDI, richiede una costante e attenta progettazione/implementazione del curricolo digitale, continuativo e trasversale alle varie discipline ed elaborato in relazione al target di riferimento (ordine e grado, classi, etc.)⁴, allo scopo di:

⁴Si rimanda alPtof dell’Istituto e alle integrazioni relative all’educazione digitale nell’ambito del curricolo verticale di educazione civica.

- far riflettere gli alunni sul potenziale delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana, allo scopo di evitare automatismi e di conseguenza atteggiamenti e comportamenti incerti. Per tale motivo si lavorerà sull'adeguata comprensione della 'grammatica' dello strumento (**dimensione tecnologica**);
- sviluppare nei discenti la capacità di ricercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità (**dimensione cognitiva**);
- far assumere atteggiamenti responsabili in relazione sia ai dati personali che altrui, usando le tecnologie per scopi eticamente accettabili e sempre nell'ottica del rispetto per gli altri (**dimensione etica**);
- far acquisire buone pratiche sociali e, pertanto, rafforzare e potenziare le abilità socio-comunicative e partecipative per maturare una consapevolezza maggiore sui doveri nei riguardi di coloro con cui si comunica online (**dimensione sociale**).

Proprio lo sviluppo della dimensione tecnologica, cognitiva, etica e sociale permette di raggiungere le competenze digitali, intese come competenze chiave, che al termine del percorso scolastico vengono individuate e certificate coerentemente con quanto normato dalla C.M. n 3, prot. n. 1235 del 13 febbraio 2015, il cui livello raggiunto è identificato dai seguenti dagli indicatori:

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

Tutte le azioni che sono e saranno attivate dal nostro Istituto per l'implemento del curricolo e delle competenze digitali faranno riferimento ai seguenti documenti:

- Piano Scuola Digitale (PNSD);
- Sillabo sull'Educazione Civica Digitale;
- Dig.Com 2.1.: 'Il quadro di riferimento per le competenze digitali dei cittadini';
- Raccomandazione del Consiglio Europeo relative alle competenze chiave per l'apprendimento (C189/9, p. 9);
- Legge n.92 del 20 agosto 2019: "Introduzione dell'insegnamento dell'educazione civica" (in particolar modo art. 5);
- Linee guida per l'insegnamento dell'educazione civica. Allegati A-B (22-06-2020).

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 obbligatoria ai sensi della L.107/2015 sia dedicata proprio all'uso e all'inserimento delle TIC nella didattica e ai temi informatici in generale. Tale formazione è svolta dall'animatore digitale e dai docenti dell'Istituto presenti nella scuola che negli anni hanno maturato conoscenze e competenze didattico-metodologiche. Tutto il corpo docente riceverà l'assistenza, gli strumenti e i mezzi per poter mettere in pratica una didattica innovativa mediante le nuove tecnologie anche attraverso le potenzialità della piattaforma Google.

Per quanto riguarda la formazione esterna, la scuola assicura tempestiva e capillare informazione su corsi, convegni e seminari relativi a tali argomenti e continuerà ad assicurare la formazione specifica sull'utilizzo delle TIC nella didattica anche attraverso i corsi organizzati dall'istituzione, dalle scuole associate nella rete dell'ambito di appartenenza, nonché il progetto S.C.AT.T.I., attraverso una formazione specifica (azione 3.1), curata dal partner MED, finalizzata alla elaborazione di UDA in ambiente digitale.

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 (come Generazioni Connesse) allo scopo di prevenire e contrastare ogni forma di discriminazione, offesa, denigrazione e lesione della dignità dell'altro, nonché bullismo e cyberbullismo. 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. Con l'azione 1.2 e 3.3 del progetto S.C.AT.T.I., inoltre, si realizzeranno incontri di aggiornamento e monitoraggio partecipato (dalla intera platea dei docenti), con l'obiettivo di elaborare procedure di tutela e salvaguardia che nascano dalla esperienza e dall'ascolto di tutti gli attori coinvolti.

2.4 - SENSIBILIZZAZIONE DELLE FAMIGLIE E INTEGRAZIONI AL PATTO DI CORRESPONSABILITÀ

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 il sito web dell'Istituto.

Allo scopo di mantenere viva l'attenzione delle famiglie su tali temi verranno valorizzate, inoltre, le opportunità di incontro e formazione per le famiglie sui temi oggetto della Policy, offerte dal territorio, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità.

Il coinvolgimento dell'intera Comunità scolastica è parte integrante del PTOF ed è una delle misure individuate nel Piano d'azione proposto a "Generazioni Connesse".

Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di smartphone, chat line e social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo.

AZIONI (da sviluppare nell'arco dell'anno scolastico)

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

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

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

CAP. 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.

La nostra scuola, pertanto, si impegna a tutelare la privacy degli/le studenti/esse e delle loro famiglie, nonché di rendere consapevoli gli studenti e le studentesse dell'importanza del diritto alla riservatezza di se stessi e degli altri. Per tale motivo, dunque, il nostro Istituto segue la normativa prevista per il trattamento dati in relazione alle specifiche finalità istituzionali e alle specifiche norme di legge e si impegna a migliorare la sicurezza e potenziare la protezione dei dati trattati attraverso un'attenta formazione dei responsabili, degli incaricati ed eventualmente sub-incaricati del trattamento, nonché delle figure coinvolte nel processo educativo.

A tal fine, l'Istituto allega alla presente ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali.

3.2 - ACCESSO AD INTERNET

- *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
- *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.*
- *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
- *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
- *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.

Per questo motivo il nostro Istituto è attento a queste tematiche e si impegna a realizzare e potenziare tutte le attività e procedure per creare ambienti di apprendimento con le caratteristiche indicate, partecipando, infatti, a bandi di implementazione e strumentazione, ad esempio, per le classi virtuali.

Nel particolare, la nostra scuola è dotata di:

- accesso internet in tutte le classi attraverso una rete WI-FI adeguata al numero di studenti e in grado di supportare il traffico dati generato da un numero elevato di utenti (gli alunni possono usufruire della connessione solo tramite pc);
- connessione ad internet tramite collegamento wireless. La Dirigenza e l'Amministrazione hanno una rete separata;
- connessione in tutte le aree della scuola;
- laboratori di informatica con software di controllo gestito dal docente.

Per quanto riguarda l'accesso ad internet, filtri, antivirus e navigazione, il nostro Istituto presenta 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.

G-SUITE FOR EDUCATION

L'Istituto “G.Caloprese” ha attivato, inoltre, i servizi della piattaforma G-Suite for Education che Google mette gratuitamente a disposizione delle scuole e delle università. Questa “Suite” è costituita da un insieme di applicazioni (la posta elettronica, documenti condivisi (Google drive), calendario, siti web (Sites) e Google Classroom (classi virtuali). Con le GSfE la proprietà dei dati rimane in capo all'utente, con totale protezione e

privacy e priva di pubblicità, mentre per gli account privati le possibilità di “intromissione” da parte di Google sono numerose. L’obiettivo di questa iniziativa è ottimizzare, attraverso le tecnologie di rete, l’attività didattica e la circolazione delle informazioni interne, come comunicazioni, documentazione e didattica (tramite uso di applicazioni specifiche). Le attività della “G-Suite for Education” consentono di gestire in modo efficace il flusso informativo all’interno dell’istituto attraverso tre strumenti principali e relative applicazioni:

- Comunicazione: Gmail, Meet, Hangouts, Calendar, gruppi Google+
- Archiviazione: Drive
- Collaborazione: Condivisione di Documenti, fogli, presentazioni, moduli, Sites e di Google Classroom per la gestione di una classe virtuale.
- ad ogni studente è stato assegnato una casella postale composta dall’iniziale del proprio nome, cognome, seguita dal nome di dominio della scuola, esempio: ncognome@icscalea.edu.it

Gli studenti, già durante la DAD, hanno utilizzato la casella di posta all’interno del dominio @icscalea.edu.it e ad uso esclusivo per le attività della scuola. Anche in quest’anno scolastico, in virtù della DDI, l’Istituto continuerà ad utilizzare i servizi offerti da GSuite for Education.

Per lavorare bene insieme si sono stabilite ovviamente delle regole di comportamento rese note attraverso la relativa liberatoria. Lo studente, infatti, riceverà la password per accedere ai servizi di Google Suite for Education solo quando lui e un suo genitore/tutore avranno sottoscritto e riconsegnato agli insegnanti le regole di utilizzo, dichiarando così di averle accettate e di essere a conoscenza della normativa locale, nazionale ed europea vigente. È solo in tal modo che lo studente avrà accesso alla piattaforma di Google Suite for Education.

Lo studente si impegna:

- ✓ a conservare la password personale e a non consentire l’uso ad altre persone;
- ✓ a comunicare immediatamente attraverso email a admin@icscalea.edu.it l’impossibilità di accedere al proprio account o il sospetto che altri possano accedervi;
- ✓ a non consentire ad altri, a nessun titolo, l’utilizzo della piattaforma Google Suite for Education;
- ✓ a non diffondere eventuali informazioni riservate di cui venissero a conoscenza, relative all’attività delle altre persone che utilizzano il servizio;
- ✓ ad osservare il regolamento, pena la sospensione da parte dell’Istituto dell’account personale dello studente,
- ✓ ad utilizzare i servizi offerti solo ad uso esclusivo per le attività didattiche della scuola.

Lo studente e la sua famiglia si assumono la piena responsabilità di tutti i dati da lui inoltrati, creati e gestiti attraverso la piattaforma Google Suite for Education.

Di conseguenza, lo studente sottoscrive anche le regole di comportamento – la cui infrazione comporterà sanzioni - affinché il servizio possa funzionare nel miglior modo possibile, tenendo presente che cortesia ed educazione, che regolano i rapporti comuni tra le persone, valgono anche in questo contesto.

Di seguito la **Netiquette** indicata nella liberatoria:

1. Poiché il servizio è uno dei mezzi di comunicazione tra Docenti e lo Studente, dovrai accedere alla piattaforma con frequenza quotidiana;
2. se utilizzi un PC non esclusivamente tuo userai sempre il software Google Chrome o Firefox in modalità NAVIGAZIONE IN INCOGNITO;
3. in POSTA e in GRUPPI invierai messaggi brevi che descrivono in modo chiaro di cosa stai parlando; indicherai sempre chiaramente l’oggetto in modo tale che il destinatario possa immediatamente individuare l’argomento della email ricevuta;
4. non inviare mai lettere o comunicazioni a catena che causano un inutile aumento del traffico in rete;
5. non utilizzare la piattaforma in modo da danneggiare, molestare o insultare altre persone;
6. non creare e non trasmettere immagini, dati o materiali offensivi, osceni o indecenti;
7. non creare e non trasmettere materiale offensivo per altre persone o enti;
8. non creare e non trasmettere materiale commerciale o pubblicitario se o espressamente richiesto;
9. quando condividi documenti non interferire, danneggiare o distruggere il lavoro dei tuoi docenti o dei tuoi compagni;

10. non curiosare nei file e non violare la riservatezza degli altri studenti;
11. usa il computer e la piattaforma Google Suite for Education in modo da mostrare considerazione e rispetto per compagni e insegnanti.

L'Istituto, dunque, in relazione alle direttive e alle indicazioni, si impegna alle seguenti azioni per la **cybersecurity**:

- Mantenere separate le reti didattica e segreteria;
- aggiornare periodicamente software e sistema operativo;
- definire la programmazione di backup periodici;
- garantire formazione adeguata allo staff, incluso il corpo docenti;
- testare regolarmente le possibili vulnerabilità;
- preparare piani di azione in risposta ai problemi più seri;
- predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo;
- impostare il browser per eliminare dei cookies alla chiusura;
- definire una policy sulla password: le password devono essere forti;
- minimizzare i privilegi amministrativi;
- sviluppare il regolamento sull'uso delle tecnologie a scuola (policy di uso accettabile).

Si allegano, inoltre, anche le 'Linee Guida in tema di privacy e sicurezza informatica' approvate dal nostro istituto all'interno del **Regolamento per lo svolgimento delle sedute collegiali in modalità telematica**.

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.

Il nostro istituto dispone dei seguenti strumenti di comunicazione:

a) Sito web della scuola

La scuola è dotata di sito internet <https://www.icscalea.edu.it/>

Il sito si configura come un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali e avvisi di carattere generale.

L'inserimento dei contenuti è possibile solo agli addetti del personale di Segreteria, per quanto riguarda i dati di tipo economico-amministrativo; alcuni docenti gestiscono le pagine descrittive dell'Istituto e delle attività che vi si svolgono.

Il personale che è in possesso delle credenziali per la gestione dei contenuti sul portale si assumerà la responsabilità editoriale di garantire che il contenuto inserito sia accurato e appropriato, anche e soprattutto ai fini del rispetto del Codice dell'Amministrazione Digitale (CAD).

b) Registro elettronico

Fra gli strumenti di comunicazione interna si annovera il registro elettronico, con tutte le sue funzionalità. Le famiglie, così, possono visualizzare molte informazioni utili, interagendo con la scuola, su:

- andamento scolastico;
- risultati scolastici (voti, documenti di valutazione);
- eventi;
- comunicazioni varie.

c) G-Suite for Education (cfr. paragrafo 3.2).

d) Strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne

In riferimento all'uso degli strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne, come avviene generalmente fra i docenti mediante ad esempio l'uso di gruppi Whatsapp o Telegram, è importante ricordare quello che si può definire "diritto alla disconnessione". L'art. 22 (Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola) del CCNL 2016/2018, infatti, fa riferimento ai criteri generali per l'utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio, al fine di una maggiore conciliazione fra vita lavorativa e vita familiare.

Lo stato emergenziale vissuto nell'a.s. 2019/2020 ha favorito la comunicazione informale fra colleghi e docenti, nonché eccezionalmente anche un primo raggiungimento degli allievi e delle famiglie, allo scopo di attivare in tempi brevi la didattica a distanza.

È importante sottolineare, però, che non esiste una vera e propria regolamentazione per la **circolazione di informazioni e di comunicazione interne** tramite gli strumenti online e, per tale ragione è fondamentale, a partire dal buon senso e da una riflessione sulle peculiarità del mezzo, predisporre comunque delle regole condivise sull'uso delle stesse, come quelle indicate di seguito:

- Mettere in chiaro fin dall'inizio, comprendere e rispettare sempre le finalità del gruppo, scrivendo e pubblicando solo contenuti pertinenti a tali finalità;
- usare sempre un linguaggio adeguato e il più possibile chiaro e preciso (come già sottolineato la comunicazione online si presta spesso a non pochi fraintendimenti);
- evitare di affrontare in chat argomenti troppo complessi e controversi (la comunicazione online in una chat di gruppo non è adatta per la gestione di problematiche di questo tipo, che certamente è più opportuno affrontare in presenza o in un Consiglio di classe);
- evitare discussioni di questioni che coinvolgono due o pochi interlocutori, onde evitare di annoiare e disturbare gli altri componenti del gruppo;
- non condividere file multimediali troppo pesanti;
- evitare il più possibile di condividere foto di studenti in chat;
- indirizzare solo domande precise e chiare, a cui si possano dare risposte altrettanto brevi e precise;
- evitare messaggi troppo spezzettati, cercando il più possibile di essere brevi ed esauritivi allo stesso tempo.

Si ricorda, inoltre, quando si usano invece chat formali, create ad esempio dal Dirigente scolastico per veicolare messaggi, informazioni e aggiornamenti relativi all'attività scolastica, la regolamentazione è prevista dalla contrattazione di Istituto.

La contrattazione di istituto al titolo VIII "CRITERI GENERALI PER L'UTILIZZO DI STRUMENTAZIONI TECNOLOGICHE DI LAVORO IN ORARIO DIVERSO DA QUELLO DI SERVIZIO, AL FINE DI UNA MAGGIORE CONCILIAZIONE TRA VITA LAVORATIVA E VITA FAMILIARE (DIRITTO ALLA DISCONNESSIONE).(art.22 comma 4 lettera C8 CCNL Scuola 2018)" stabilisce che:

Art. 34 Tipologia e modalità di comunicazione.

Gli strumenti elettronici per la comunicazione si distinguono in strumenti sincroni e asincroni. I primi, a differenza dei secondi, richiedono che entrambi i terminali della comunicazione (trasmittente e ricevente) siano connessi perché si abbia comunicazione.

La comunicazione telefonica tradizionale richiede la connessione tra chi trasmette e chi riceve.

La messaggistica (whatsapp, mail, messenger) può avvenire anche se una delle due parti non è connessa, in questo caso chi riceve decide tempi e modalità di consultazione dei messaggi ricevuti.

Art. 35 Modalità e tempi di convocazione e delle comunicazioni ufficiali.

Le convocazioni ufficiali degli organi collegiali, degli incontri scuola famiglia, degli organi tecnici devono avvenire con comunicazione scritta, pubblicata nel sito web della scuola, con i giorni di preavviso previsti per legge o dai regolamenti.

Le comunicazioni pubblicate nel sito web devono essere consultate e lette dai docenti e dal personale ATA.

Le richieste di adempimenti e le convocazioni fissate per il giorno della ripresa delle attività didattiche, dopo un periodo di vacanza, non possono essere pubblicate il giorno precedente il periodo festivo stesso.

Art. 36 Diritto alla disconnessione.

Questo strumento contrattuale vuole tutelare la conciliazione tra vita lavorativa e vita familiare, così si eliminano l'invasività del datore di lavoro e l'obbligo per il lavoratore di rimanere connessi 24 ore su 24 e 7 giorni su 7: la contrattazione integrativa stabilisce che il dirigente scolastico e la scuola potranno fornire informazioni telefoniche e messaggistiche ai dipendenti dalle 08.00 alle 14.00 e dalle 15.30 alle 18.00.

Art. 37 Modalità e tempi di utilizzo delle comunicazioni sincrone (telefoniche).

I lavoratori non possono essere contattati telefonicamente per problematiche riguardanti la prestazione lavorativa durante il periodo di sospensione delle attività didattiche e nei periodi festivi.

I collaboratori del dirigente scolastico, le funzioni strumentali e responsabili di plesso, i docenti che hanno compiti organizzativi, in caso d'urgenza, possono essere contattati anche fuori dai suddetti limiti temporali.

Nei limiti dell'orario di funzionamento degli uffici di segreteria e di presidenza è possibile contattare i lavoratori durante il periodo di sospensione delle attività didattiche per comunicazioni connesse al proprio stato giuridico o economico.

Per ragioni di sicurezza ed emergenza i suddetti limiti sono superati al fine di evitare o prevenire situazioni di pericolo.

Art. 38 Modalità e tempi di utilizzo delle comunicazioni asincrone (messaggistica).

La comunicazione tramite i "canali sociali" non richiedono la connessione contestuale e contemporanea dei lavoratori. In questo caso è possibile inviare comunicazioni anche in periodi non lavorativi poiché è garantita la piena libertà del lavoratore di scegliere i tempi di lettura e di replica. A tal fine, trattandosi di trasmissione di messaggi, che non richiedono la connessione contemporanea, i lavoratori (tra questi è incluso anche il dirigente scolastico) possono decidere i tempi di trasmissione dei messaggi, fatto salvo il diritto di chi riceve di leggere e replicare nei tempi desiderati.

In ogni caso le comunicazioni a mezzo dei canali sociali informatici con gli utenti e con i colleghi devono essere finalizzate ad informazioni di servizio e alle interazioni necessarie per lo svolgimento della funzione di educazione, di istruzione e di orientamento.

3.4 - STRUMENTAZIONE PERSONALE

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/le 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.

Per tale ragione, l'Istituto si impegnerà ad attivare, in contesti di totale sicurezza, l'utilizzo dei dispositivi 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").

La presente **ePolicy** contiene indicazioni e integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, prevedendo misure per prevenire tipologie di rischio (non solo come quelle più frequenti come il cyberbullismo) e stabilire procedure specifiche per rilevare e gestire le diverse problematiche. Risulta fondamentale, pertanto, per la nostra 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 sia i lati positivi che eventuali criticità nella e per la didattica.

Di seguito è indicato come l'utilizzo della strumentazione personale è regolamentata all'interno del nostro Istituto.

PER LA COMPONENTE STUDENTESCA

- ✓ I telefoni cellulari, i tablet e le relative fotocamere e registratori vocali non verranno utilizzati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate dal corpo docente.
- ✓ L'insegnante della prima ora ricorda agli alunni di spegnere i cellulari (si rimanda al Regolamento d'Istituto che disciplina le diverse sanzioni per l'uso improprio del dispositivo mobile).

- ✓ Alunni con disturbi specifici di apprendimento, 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.
- ✓ Giochi e console, tra cui la Sony Playstation, Microsoft Xbox e similari, che possono avere accesso a Internet non filtrato, non sono consentiti nemmeno se custoditi come previsto per gli altri dispositivi. Saranno requisiti dal docente che ravvisa l'infrazione, depositati in dirigenza e consegnati al genitore/tutore convocato, che sarà contestualmente informato dell'eventuale sanzione disciplinare comminata al trasgressore.
- ✓ 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 a un operatore; allo stesso modo le famiglie devono chiamare il centralino della scuola se hanno assoluta necessità di parlare con i 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.

PER IL PERSONALE DOCENTE/ATA

- ✓ 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 espressamente programmate.
- ✓ La password di accesso alla rete va custodita con cura e per nessuna ragione deve essere divulgata a chi non ha titolo per utilizzarla (studenti, genitori, operatori esterni).
- ✓ 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.

UTILIZZO DEL LABORATORIO DI INFORMATICA E DELLA POSTAZIONI DI LAVORO

La scuola è già dotata di un regolamento di fruizione e di utilizzo del laboratorio di informatica che si configura come allegato alla presente. Tuttavia è utile, in questa Policy, ricordare le disposizioni generali sull'uso dei laboratori:

1. Le apparecchiature presenti nella scuola sono patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.
2. I laboratori informatici e le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.
3. Quando un insegnante, da solo o in classe, usufruisce del laboratorio deve registrare il proprio nome e l'eventuale classe nell'apposito registro delle presenze di laboratorio, indicando il numero della postazione utilizzata. Questo allo scopo di poter risalire alle cause di eventuali inconvenienti o danneggiamenti e per comprovare l'effettivo utilizzo dell'aula.

4. L'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante.
5. Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software.
6. Nei laboratori è vietato utilizzare CD personali o altri dispositivi se non dopo opportuno controllo con sistema di antivirus aggiornato.
7. All'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il locale in ordine e le macchine spente correttamente
8. In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile del laboratorio.
9. 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.

Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

AZIONI (da sviluppare nell'arco dell'anno scolastico)

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

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

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

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

CAP. 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 che adotteremo per poter ridurre l'incidenza di situazioni di rischio si configurano come interventi di **sensibilizzazione e prevenzione**.

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

4.2 - CYBERBULLISMO: CHE COS'È E COME PREVENIRLO

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

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

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

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;

- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
 - ✓ Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
 - ✓ Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

4.3 - HATE SPEECH: CHE COS'È E COME PREVENIRLO

Il fenomeno di “incitamento all'odio” o “discorso d'odio”, indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine “hate speech” indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

Il nostro Istituto, in relazione a questa problematica, intende sensibilizzare la comunità scolastica attraverso attività di analisi e riflessione, in un'ottica trasversale e interdisciplinare, avvalendosi anche dell'aiuto e del supporto del materiale presente sul sito di Generazioni Connesse, nonché organizzando interventi con enti e associazioni del territorio.

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.

Il nostro Istituto, per prevenire tali fenomeni, intende sensibilizzare la comunità scolastica attraverso azioni di prevenzione che abbiano come oggetto il benessere digitale, in un'ottica trasversale e interdisciplinare, ricorrendo anche al materiale presente sul sito di Generazioni Connesse, nonché programmando interventi con enti e associazioni del territorio.

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.

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).

Il nostro Istituto, per prevenire tali fenomeni, intende sensibilizzare la comunità scolastica attraverso azioni di analisi e riflessione, nonché percorsi di educazione all'affettività ed educazione digitale, in relazione comunque al target di riferimento, in un'ottica trasversale e interdisciplinare, avvalendosi anche dell'aiuto e del supporto del materiale presente sul sito di Generazioni Connesse, nonché organizzando interventi con enti e associazioni del territorio che coinvolgano anche i genitori allo scopo di attivare forme di controllo parentale relative alla navigazione in rete.

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, anche per questa tematica estremamente delicata, si attiveranno percorsi e riflessioni guidate 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.

La scuola si impegna a creare anche attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: si ricorda, inoltre, che è possibile e opportuno segnalare

eventuale materiale pedopornografico, 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.

AZIONI (da sviluppare nell’arco dell’anno scolastico)

- ✓ Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- ✓ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all’utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.
- ✓ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all’utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- ✓ Organizzare uno o più incontri di formazione all’utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.
- ✓ Promuovere incontri e laboratori per studenti e studentesse dedicati all’ Educazione Civica Digitale.
- ✓ Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.
- ✓ Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull’inclusione rivolti a genitori, studenti/studentesse e personale della scuola.
- ✓ Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

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

- ✓ Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- ✓ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all’utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.
- ✓ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all’utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.
- ✓ Organizzare uno o più incontri di formazione all’utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.
- ✓ Promuovere incontri e laboratori per studenti e studentesse dedicati all’ Educazione Civica Digitale.
- ✓ Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.
- ✓ Organizzare laboratori di educazione alla sessualità e all’affettività, rivolti agli/lle studenti/studentesse.
- ✓ Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull’inclusione rivolti a genitori, studenti/studentesse e personale della scuola.
- ✓ Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

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, si ricorda che, secondo, la normativa 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.

Si ricordano, 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 si rimanda 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:

- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- docente referente per le segnalazioni.

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

5.3 - GLI ATTORI SUL TERRITORIO

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

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

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

- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell’infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale:** supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all’uso di Internet.
- **Polizia Postale e delle Comunicazioni:** accoglie tutte le segnalazioni relative a comportamenti a rischio nell’utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali:** forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l’Infanzia e l’Adolescenza e Difensore Civico:** segnalano all’Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.
- **Focal point Child Safeguarding Policy di Save the Children (tramite Punto Luce Scalea).**
- **Focal Point Child Safeguarding Policy di EDI (tramite ASS. Gianfrancesco Serio - prog. S.C.AT.T.I.).**

Procedure interne: cosa fare in caso di evidenza di Cyberbullismo

Il docente ha evidenza che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Avvisa il referente per il cyberbullismo (e/o il referente indicato nell'ePolicy) e il Dirigente Scolastico che convoca il CDC.

A) Se c'è fattispecie di reato - seguite le procedure della scuola

B) Se non c'è fattispecie di reato

- Richiedi la consulenza dello psicologo/a scolastico

- Informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto), se possibile con la presenza dello psicologo/a, su quanto accade e condividete informazioni e strategie.

- Informa i genitori di ragazzi/e infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy)

- Attiva il consiglio di classe.

- Valuta come coinvolgere gli operatori scolastici su quanto sta accadendo.

Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

NELLE CLASSI

- Cerca di capire il livello di diffusione dell'episodio nell'Istituto e parla della necessità di non diffondere ulteriormente online i materiali.

- Parla del cyberbullismo e delle sue conseguenze (non nominare gli alunni coinvolti). Suggestisci di chiedere aiuto per situazioni di questo tipo. Prevedi un momento laboratoriale in modo da facilitare l'elaborazione della situazione.

- a seconda della situazione trova il modo di supportare la vittima e di responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.

A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnala alla Polizia Postale:

a) contenuto; b) modalità di diffusione.

Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo

Il docente sospetta che stia accadendo qualcosa tra gli studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Sonda il clima di classe, ascoltando i ragazzi e monitorando ciò che accade (ma senza fare indagini o interrogatori). Cerca di capire il livello di diffusione dell'episodio a livello di Istituto.

Parla in classe del cyberbullismo e delle sue conseguenze (non nominare gli alunni che sospetti coinvolti). Suggestisci di chiedere aiuto per situazioni di questo tipo. Proponi attività in classe sull'empatia e sul riconoscimento delle emozioni (proprie e altrui)

Se emergono evidenze passa allo schema successivo

Condividi con il referente per il cyberbullismo (e/o il referente indicato nell'e-policy): valuta con lui/loro le possibili strategie di intervento.

Valuta se è il caso di avvisare il consiglio di classe.

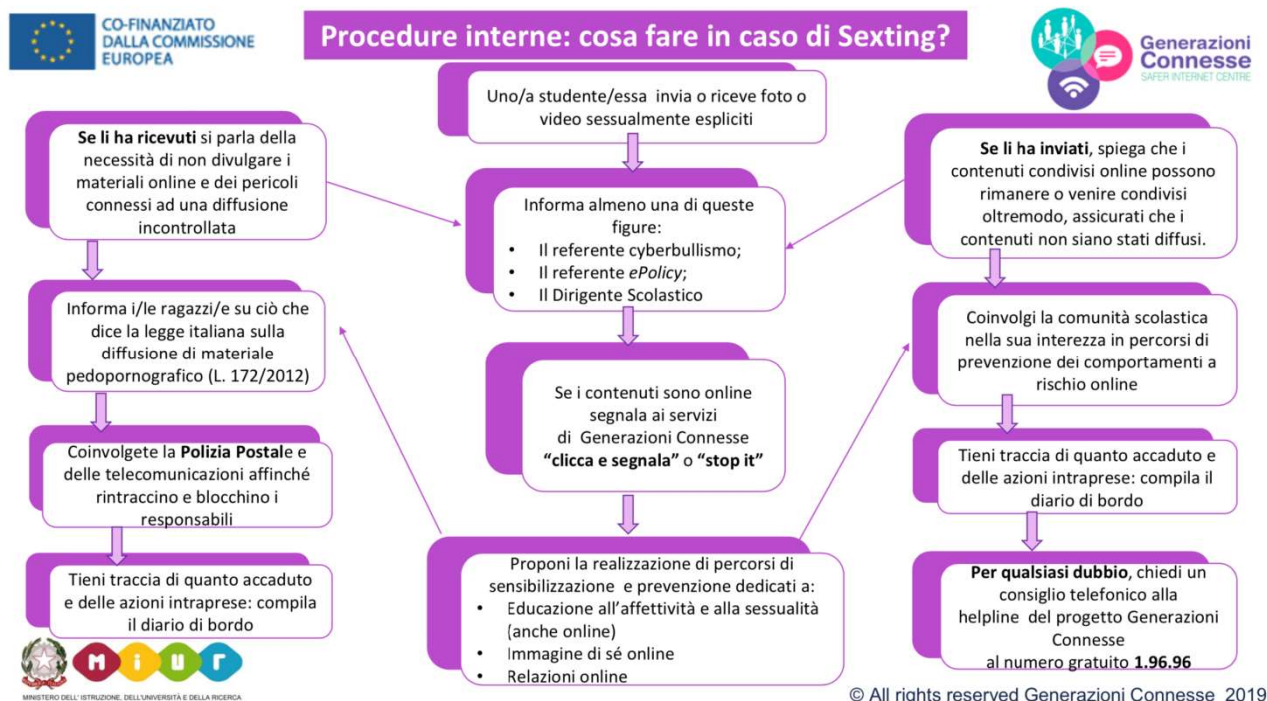
Valuta se è il caso di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.

Informa i/le ragazzi/e su ciò che dice la legge italiana su cyberbullismo L. 71/2017) Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

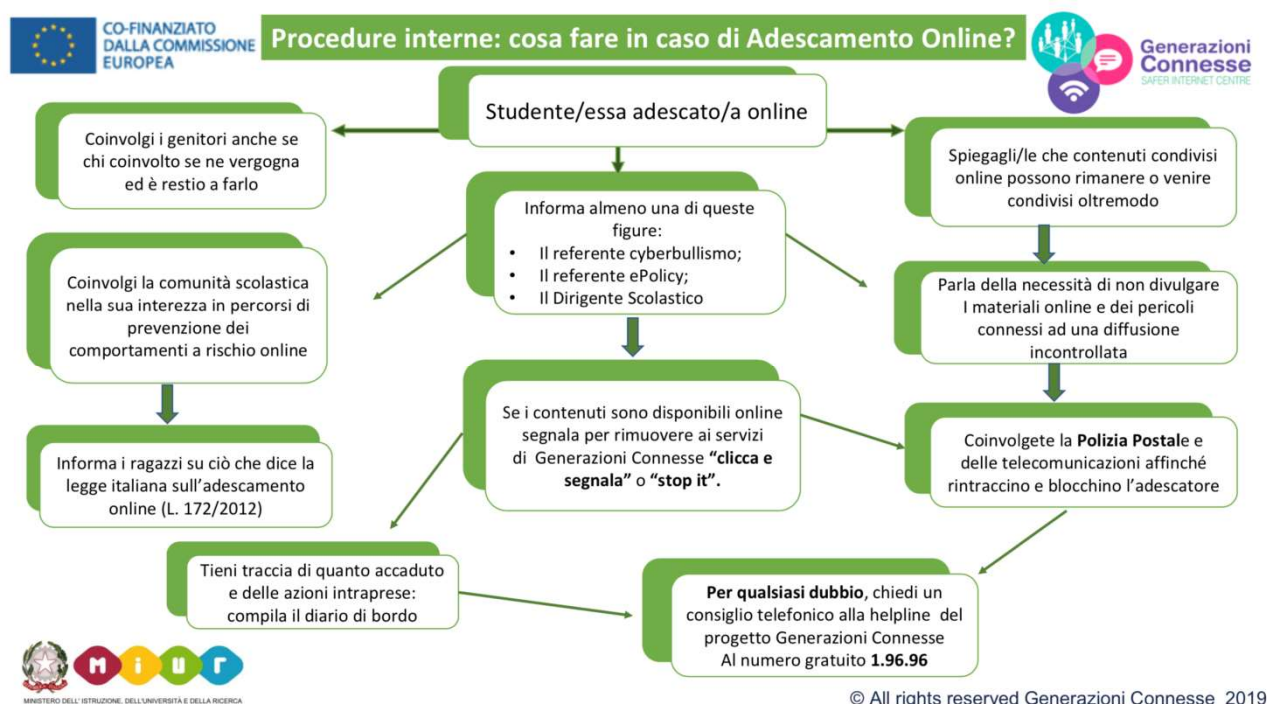
Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Ricorda a studenti/esse che possono chiedere in qualsiasi momento una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 o via chat

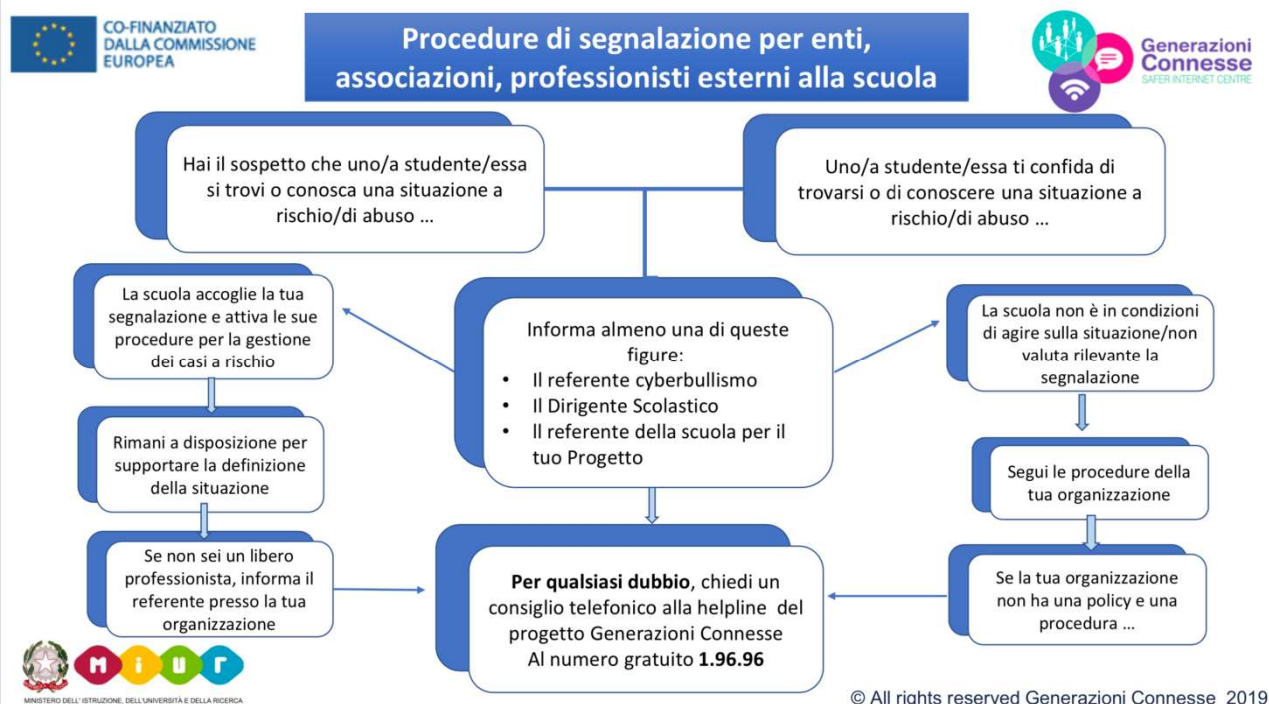
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



MODULO PER LA SEGNALAZIONE DI CASI

Nome di chi compila la segnalazione:	Ruolo:
Data:	Scuola:

Descrizione dell'episodio o del problema			
Soggetti coinvolti	Vittima/e: 1..... Classe: 2..... Classe: 3..... Classe:	Autore/autrice e sostenitori: 1..... Classe: 2..... Classe: 3..... Classe:	
Chi ha riferito dell'episodio?	- La vittima - Un compagno della vittima, nome: - Genitore, nome: - Insegnante, nome: - Altri, specificare:		
Atteggiamento del gruppo	Da quanti compagni è sostenuto il bullo? Quanti compagni supportano la vittima o potrebbero farlo?		
Gli insegnanti sono intervenuti in qualche modo ?			
La famiglia o altri adulti hanno cercato di intervenire ?			
Chi è stato informato della situazione?	☐ coordinatore di classe ☐ consiglio di classe ☐ dirigente scolastico ☐ la famiglia della vittima/e	data: data: data: data:	☐ la famiglia del bullo/i ☐ le forze dell'ordine ☐ altro, specificare:

MODULO PER IL FOLLOW-UP DEI CASI

	AZIONI INTRAPRESE	La situazione è
Aggiornamento 1		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 2		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 3		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 4		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 5		☐ migliorata ☐ invariata ☐ peggiorata Come:

Schema riepilogativo delle situazioni gestite legate a rischi online

[illegible]