ISTITUTO COMPRENSIVO STATALE - -CALIMERA
Prot. 0002281 del 29/06/2020
01 (Uscita)

Documento di ePolicy

LEIC816004

I.C. CALIMERA

VIA UGO FOSCOLO N.1 - 73021 - CALIMERA - LECCE (LE)

PIERA LIGORI

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

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

5. Gestione delle infrazioni alla ePolicy
6. Integrazione dell'ePolicy con regolamenti esistenti
7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

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

Perché è importante dotarsi di una E-policy?

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

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

Introduzione

I Nuovi Media mettono a disposizione diverse opportunità di relazione e di comunicazione; aprono

ad un mondo di emozioni, di scambio di informazioni e di apprendimento che offre, in particolare ai giovani, occasioni di crescita senza precedenti. I ragazzi di oggi sono nativi digitali. Considerano le tecnologie come elemento naturale del loro ambiente di vita al punto di provare, come afferma Papert, un naturale innamoramento per la tecnologia. Nelle loro case e nelle loro camerette, sono sempre più presenti consolle per i videogiochi, cellulari, computer, iPod, tablet, insieme a esperienze di intrattenimento, socializzazione vissute attraverso Internet e i social network. I Nuovi Media, inoltre, presentano un approccio alla conoscenza e ai saperi non lineare, ma reticolare e in modo multitasking: si studia mentre si ascolta musica e, nello stesso tempo, si mantengono in contatto con gli amici attraverso MSN, Facebook, whatsapp ….ecc. La didattica non può rimanere indietro rispetto alla tecnologia, che deve entrare nella scuola, ma deve essere funzionale all'obiettivo che ci siamo dati e al percorso che vogliamo fare per raggiungerlo. La tecnologia è utile se fa crescere i ragazzi e la comunità. Il mondo digitale e virtuale rappresenta, dunque, un'enorme opportunità di sviluppo e di crescita culturale e sociale, ma nasconde altresì una serie di insidie e pericoli, all'interno e al di fuori della scuola, cui occorre far fronte: siamo infatti di fronte ad una realtà complessa, apparentemente priva di regole, nella quale trovano spazio contenuti e comportamenti potenzialmente dannosi per lo sviluppo dei più giovani, derivanti da un uso non consapevole e responsabile delle tecnologie digitali da parte di bambini/e, ragazzi e ragazze. Contro i rischi online (adescamento online, cyberbullismo, sexting, violazione della privacy, pornografia, pedopornografia, gioco d'azzardo o gambling,, dipendenza da internet, videogiochi online esposizione a contenuti dannosi o inadeguati, dipendenza da shopping online) è essenziale, costruire la resilienza degli allievi ai rischi a cui possono essere esposti, in modo che abbiano la fiducia e le competenze per affrontare al meglio questi pericoli. Gli adulti hanno un ruolo fondamentale nel garantire che bambini/e e adolescenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato e sicuro, ruolo che vede coinvolti a pieno titolo tutti coloro che hanno un ruolo educativo, oltre che formativo, genitori inclusi. È in questo quadro che la nostra scuola ha scelto di inserire nel Piano triennale dell'Offerta Formativa, il progetto "Generazioni Connesse" dotando la comunità scolastica della seguente e-safety , quale strumento concreto a ricevere informazioni utili, a prevenire certe situazioni di rischio e a gestirle al meglio nel caso si verifichino.

Scopo della Policy

Scopo del presente documento è quello di definire :

• le misure finalizzate alla prevenzione nella scuola di fenomeni legati ai rischi delle tecnologie digitali

• le misure atte a facilitare e promuovere l'utilizzo corretto e responsabile delle TIC nella didattica e negli ambienti scolastici

• le modalità di accesso e di uso della Rete informatica, telematica e dei servizi nel rispetto della normativa vigente

• l' uso consapevole della navigazione ed il riconoscimento dei rischi connessi alla stessa

• le misure per la segnalazione dei casi

• le misure per la gestione dei casi

1.2 - Ruoli e responsabilità

Affinché l'E-policy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, s'impegni nell'attuazione e promozione di essa.

Il Dirigente scolastico deve:

- garantire l'e-sicurezza nella scuola

- in caso di infrazioni, intervenire per via amministrativa secondo le norme vigenti previste dal regolamento d'Istituto

L'Animatore Digitale deve:

- guidare la scuola nella digitalizzazione

- promuovere progetti innovativi

- offrire nuove opportunità per diffondere la cultura della e-sicurezza in tutto l'Istituto

Il Personale docente deve:

- educare con i media (identità, privacy, credibilità, partecipazione, creatività)

- promuovere e sostenere comportamenti sicuri nelle loro classi, seguendo le procedure di e-sicurezza della scuola ed educando in tal modo gli alunni ad un uso critico e consapevole di Internet anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose

- favorire una cultura 'No Blame' (non colpevole), in modo che gli allievi si sentano in grado di segnalare qualsiasi situazione di bullismo, abuso o materiali inadatti

- essere responsabili delle strumentazioni informatiche in dotazione alla scuola, segnalando eventuali danni e/o anomalie

- responsabilizzare gli alunni per divenire consapevoli dell'importanza della salvaguardia di un bene comune, seguendo le corrette norme di utilizzo

- far conoscere la e-safety a tutti gli studenti e ai genitori all'inizio di ogni nuovo anno scolastico insieme al Patto di Corresponsabilità

Resta fermo che non è possibile garantire una navigazione totalmente priva di rischi e che la Scuola e gli insegnanti non possono assumersi le responsabilità conseguenti all'accesso accidentale a siti illeciti o al reperimento ed uso di materiali inappropriati.

Gli alunni devono:

- prendere parte attiva alle attività previste per affrontare le questioni di e-sicurezza sia a casa che a scuola

- accettare una serie di linee guida e regole che riguardano le loro responsabilità quando si utilizzano le TIC a scuola.

I genitori devono:

- condividere regole comuni (da inserire nel patto di corresponsabilità educativa) per l'utilizzo sicuro di Internet sia a casa sia a scuola

- vigilare a casa per un uso corretto di Internet

- impegnarsi ad utilizzare i social network dei gruppi classe dei genitori, per facilitare la comunicazione scuola-famiglia, evitando dannose strumentalizzazioni

- essere consapevoli che i gruppi WhatsApp-genitori non possono essere usati per deresponsabilizzare i propri figli nella gestione dei compiti a casa o per gestire livelli comunicativi che invadono il campo della didattica o mettano in discussione la libertà d'insegnamento

- raggiungere un'alleanza scuola-famiglia che abbia al centro i bambini e non sia genitocentrica, per perseguire obiettivi comuni . Ai genitori sono date informazioni sulla politica e la sicurezza della scuola durante gli incontri scuola famiglia, attraverso incontri-dibattiti con esperti e Focus Group sui rischi online.

Il Personale ATA deve:

- essere di supporto all'azione didattica

- collaborare per l'efficienza e l'efficacia del servizio legato alla sicurezza e/o e-sicurezza a scuola

---

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).

Alla stipula del contratto, la scuola fa sottoscrivere un'informativa per i soggetti esterni che erogano attività educative nell'Istituto in cui si impegnano al rispetto delle norme sulla privacy relativamente a fatti, informazioni e dati sensibili di cui dovessero venire a conoscenza nel corso del loro incarico.

Durante lo svolgimento del proprio incarico i soggetti esterni sono tenuti a rispettare i regolamenti che ordinariamente valgono per tutto il personale interno operante nella scuola.

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

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

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

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

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

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

L'E-policy sarà condivisa e comunicata attraverso:

- Sito web della scuola

- Focus group tra studenti

- Focus group tra docenti

- Incontri con il personale ATA

- Incontri con i genitori

- Incontri pubblici con i rappresentanti delle Istituzioni del territorio

- Patto di corresponsabilità

1.5 - Gestione delle infrazioni alla ePolicy

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

La gestione delle infrazioni alla Policy spetta al dirigente scolastico in sinergia con i Consigli di Classe/interclasse/sezione e, per i casi particolari, con l'Organo di Garanzia.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

Il presente documento è integrato con i regolamenti scolastici attualmente in vigore nell'Istituto:

"Regolamento d'Istituto", "Patto educativo di corresponsabilità", " Linee guida DAD" consultabili al link "Regolamenti" del sito della scuola (Regolamento di Istituto, http://www.icscalimera.gov.it/regolamento-di-istituto/).

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

Il nostro Istituto monitora l'implementazione della eSafety attraverso le seguenti azioni:

- presentazione ufficiale della e-Safety nei Consigli di classe/interclasse/ intersezione

- presentazione ai genitori degli alunni che iniziano per la prima volta il percorso scolastico

- rilevazione del numero dei download della e-Safety dal sito della scuola

- questionario finale per genitori, docenti e alunni sull'applicazione delle norme della e-Safety

- rilevazione del numero dei casi di infrazione per anno scolastico (Diario di Bordo).

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti
- Organizzare 1 evento di presentazione del progetto Generazioni Connesse rivolto ai genitori
- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto ai docenti

Azioni da svolgere nei prossimi 3 anni:

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

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali".

Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico" ("Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente", C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale.

Il Curricolo della nostra Scuola prevede l'utilizzo delle TIC da parte degli insegnanti e da parte degli alunni come parte integrante della didattica. Negli ultimi anni la scuola ha cercato di dotarsi di strumenti tecnologici attraverso i progetti PON_FESR (LIM nelle classi, laboratori multimediali e linguistici...) e di favorire la formazione del personale per far crescere le competenze professionali nell'impiego delle nuove tecnologie.

Il Curricolo Verticale è stato redatto facendo riferimento al testo delle Indicazioni Nazionali per il curricolo del 2012 e agli orientamenti emersi a livello europeo (Competenze chiave per l'apprendimento permanente, 22 maggio 2018) e ai documenti italiani (Indicazioni Nazionali e Nuovi scenari, 2018).

Nel Curricolo Verticale la competenza digitale è trasversale ad ogni campo di esperienza e disciplina e viene declinata in conoscenze, abilità, atteggiamenti, esperienze formative che sviluppano tale competenza in modo trasversale.

CURRICOLO COMPETENZE CHIAVE (RACCOMANDAZIONE DEL CONSIGLIO EUROPEO DEL 22 MAGGIO 2018 RELATIVA ALLE COMPETENZE CHIAVE PER L'APPRENDIMENTO PERMANENTE)

Competenze digitale

Definizioni

La competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza, spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Comprende l'alfabetizzazione informatica e digitale, Ia comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitaìi (inclusa la programmazione), la sicurezza (compresa la cibersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico.

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, oltre a 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 ed 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.

- Essere capaci di utilizzare, accedere a, filtrare, valutare, creare, programmare e condividere contenuti digitali.

- Essere in grado di gestire e proteggere informazioni, contenuti, dati e identità digitali, oltre a riconoscere software, dispositivi, intelligenza artificiale o robot e interagire efficacemente con essi.

ATTEGGIAMENTI ESSENZIALI LEGATI A TALE COMPETENZA

Interagire con tecnologie e contenuti digitali con un 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.

ESPERIENZE FORMATIVE CHE SVILUPPANO LE COMPETENZE TRASVERSALI

Campi d'esperienza: Tutti

Discipline di riferimento: Tutte, Tecnologia, Informatica

SCUOLA DELL'INFANZIA: Coding

SCUOLA PRIMARIA E SECONDARIA: Generazioni Connesse , Coding, DM/8, Musica 2.0, Pon di Cittadinanza Digitale, Etwinning, pigreco day, STEM

Il DigComp, in particolare, con le 5 aree di competenza, è diventato un riferimento per lo sviluppo e la pianificazione strategica del Curricolo sulle competenze digitali nei tre ordini di scuola.

1 Alfabetizzazione su informazioni e dati

1.1 Navigare, ricercare e filtrare dati, informazioni e i contenuti digitali

1.2 Valutare dati, informazioni e contenuti digitali

1.3 Gestire dati, informazioni e contenuti digitali

2. Comunicazione e collaborazione

2.1 Interagire con gli altri attraverso le tecnologie digitali

2.2 Condividere informazioni attraverso le tecnologie digitali

2.3 Esercitare la cittadinanza attraverso le tecnologie digitali

2.4 Collaborare attraverso le tecnologie digitali

2.5 Netiquette

2.6 Gestire l'identità digitale

3. Creazione di contenuti digitali

3.1 Sviluppare contenuti digitali

3.2 Integrare e rielaborare contenuti digitali

3.3 Copyright e licenze

3.4 Programmazione

4. Sicurezza

4.1 Proteggere i dispositivi

4.2 Proteggere i dati personali e la privacy

4.3 Proteggere la salute e il benessere

4.4 Proteggere l'ambiente

5. Risolvere problemi

5.1 Risolvere problemi tecnici

5.2 Individuare fabbisogni e risposte tecnologiche

5.3 Utilizzare in modo creativo le tecnologie digitali

5.4 Individuare i divari di competenze digitali

Il Curricolo è consultabile al seguente link

https://www.icscalimera.edu.it/curricolo-verticale-e-didattica/

2.2 - Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

Il nostro Istituto promuove numerose azioni formative e aggiornamento del personale docente con la RETE di AMBITO o con altre Reti e internet guidati dall'Animatore Digitale, dal responsabile del cyberbullismo e funzione strumentale area 2 didattica e formazione.

Nell'arco del triennio 2019-2022, la nostra scuola intende promuovere esperienze formative

coerentemente con le priorità formative individuate nel piano di miglioramento del RAV e con le azioni del PNSD riguardo la Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica, con particolare riferimento alla cittadinanza digitale. Con l'introduzione della Didattica a distanza la scuola si è dotata di specifiche linee guida per la DAD e ha supportato i docenti di ogni ordine di scuola con una formazione costante circa l'utilizzo delle piattaforme implementate (Argo didup, Edmodo, Gsuite) tramite videotutorial inseriti in una sezione del sito della scuola appositamente predisposta. Sono stati effettuati anche momenti di formazione in modalità sincrona attraverso Meet.

ESPERIENZE FORMATIVE INTERNE

Area	Risultati attesi	Destinatari
SPAZI E AMBIENTI PER L'APPRENDIMENTO	Implementare l'utilizzo dell'atelier creativo della scuola come spazio attrezzato per la partecipazione attiva degli studenti che permetta di agire le competenze chiave per l'apprendimento permanente.	Docenti interessati della scuola dell'Infanzia, Primaria e Secondaria di I grado
AMMINISTRAZIONE DIGITALE	- Utilizzare il Registro Elettronico in particolare sulla valutazione degli apprendimenti, del livello globale di maturazione, la rilevazione dei progressi, il giudizio di valutazione del comportamento, le operazioni di scrutinio e sulla certificazione delle competenze. - Saper utilizzare le nuove funzioni introdotte da Argo Didup per la gestione della didattica a distanza (bacheca, condivisione documenti,...)	Docenti della scuola Primaria e Secondaria di I grado
INNOVAZIONE DIDATTICA	-Integrare nella didattica quotidiana le potenzialità delle TIC e le risorse multimediali. -Saper utilizzare il coding per generare saperi, abilità e competenze sia disciplinari che trasversali. -Acquisire strumenti concreti per promuovere un uso sicuro e responsabile di Internet e dei Nuovi Media da parte dei più giovani. -Costruire ambienti di apprendimento: organizzare e gestire gli spazi e i tempi di insegnamento e apprendimento mediante le tecnologie e le app in una didattica digitale integrata per condividere le risorse con e tra gli studenti.	Docenti di scuola dell'Infanzia, Primaria e Secondaria di I grado
INNOVAZIONE DIDATTICA	- Sviluppare percorsi innovativi di Ricerca-Azione finalizzati a migliorare i processi di insegnamento/ apprendimento. - Implementare innovazioni didattiche da sperimentare nei vari ambiti disciplinari con un'attenzione particolare allo sviluppo delle competenze logico matematiche attraverso l'utilizzo di piattaforme digitali dedicate: STEAM e PiGreco.	Docenti di scuola Primaria e Secondaria
INNOVAZIONE DIDATTICA	- Saper gestire "Classi virtuali" per realizzare lezioni innovative digitali utilizzando gli strumenti e i contenuti disponibili sulla piattaforma EDMODO, CODE.ORG, il TWINSPACE , CLASSROOM e GSUITE, la BACHECA DIDUP.	Docenti di scuola Primaria e Secondaria di I grado
RAFFORZARE LA FORMAZIONE INIZIALE SULL'INNOVAZIONE DIDATTICA	-Sviluppare competenze didattico-musicali innovative ed inclusive da attivare nella pratica corale e strumentale secondo il D.M. 8/11, la musica d'insieme e nei percorsi di Musica 2.0 da attivare anche a distanza. -Conoscere e saper applicare il metodo "Stregati dalla musica" nel teatro musicale; saper applicare nella didattica le innovazioni digitali per la musica sperimentate nel PON inclusione.	Docenti di scuola Primaria e Secondaria di I grado.

RAFFORZARE LA FORMAZIONE INIZIALE SULL'INNOVAZIONE DIDATTICA	L'Istituto Comprensivo Calimera si è adeguato al GDPR (General Data Protection Regulation), il Regolamento attraverso il quale la Commissione Europea intende rafforzare la protezione dei dati personali di cittadini dell'Unione Europea, entrato in vigore il 25 Maggio 2018. Nel triennio 2019-22 verranno attivati momenti formativi interni/esterni coerenti con il GDPR	Personale docente

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

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

Nell'ottica di creare ulteriore sinergia fra scuola, studenti/studentesse e famiglie, di promuovere la condivisione di buone pratiche nell'utilizzo consapevole delle TIC e di prevenire e contrastare ogni forma di discriminazione, offesa, denigrazione e lesione della dignità dell'altro, nonché fenomeni di bullismo e cyberbullismo, la scuola organizza percorsi formativi specifici per i docenti .

La nostra scuola incoraggia anche percorsi di autoaggiornamento personali o collettivi, iniziative seminariali con professionisti-esperti interni attraverso il supporto dell'Animatore digitale e del team per l'Innovazione digitale ed esterni alla scuola, giornate-settimane di approfondimento in accordo con la rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc…), le amministrazioni comunali, i servizi socio-educativi e le associazioni/enti presenti. Tali azioni programmatiche sono inserite nel Piano triennale dell'offerta formativa.

Nel corso dell'anno scolastico e in occasione di eventi come il Safer Internet Day vengono organizzati momenti formativi di approfondimento (progetti specifici, laboratori, eventi, giornate, etc, …) con la famiglia e gli/le studenti/studentesse in modo da sensibilizzare l'intera comunità educante su un corretto uso delle tecnologie digitali e sulle potenzialità della Rete.

La formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali segue il seguente cronoprogramma che considera il triennio scolastico, in un'ottica di vera e propria programmazione, con azioni specifiche:

1. Analisi del fabbisogno formativo degli insegnanti sull'uso sicuro della Rete
2. Promozione della partecipazione dei docenti a corsi di formazione con oggetto i temi del progetto "Generazioni Connesse" e implementazione della E-Safety Policy
3. Monitoraggio delle azioni svolte per mezzo di specifici momenti di valutazione
4. Organizzazione incontri con professionisti della scuola o con esperti esterni, enti/associazioni, etc.

Con l'introduzione della Didattica a distanza, sebbene forzata, i docenti hanno avuto modo di misurarsi con il problema della sicurezza e della privacy che ha determinato una maggiore consapevolezza dei rischi legati all'utilizzo di internet e delle TIC; tale consapevolezza si rafforzerà nel passaggio da una didattica a distanza forzata a una didattica a distanza scelta come opportunità di arricchimento dell'offerta didattica.

Sul sito istituzionale della scuola, nell'area PNSD, è predisposto uno spazio specifico con materiali formativi per gli insegnanti. Nella sezione, sono fruibili materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di Internet, nell'ottica di condivisione fra gli insegnanti.

Sempre sul sito istituzionale della scuola, è accessibile il link ai materiali informativi del progetto di Istituto"Generazioni connesse" e al sito http://www.generazioniconnesse.it dove è possibile trovare ulteriori approfondimenti, spunti aggiornamenti e strumenti didattici utili da usare con gli studenti e le studentesse, per ciascun ordine di scuola.

Sempre sul sito istituzionale della scuola, è predisposto uno spazio specifico per la Didattica a Distanza https://www.icscalimera.edu.it/fuoriclsse/ che prevede una selezione di sitografia utile e affidabile per una didattica anche fuori dalle aule fisiche, strumenti ed esempi di buone pratiche, tutorial di supporto, contenuti multimediali per lo studio, piattaforme certificate per la didattica a distanza.

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

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

La nostra scuola attribuisce molta importanza al coinvolgimento delle famiglie nell'educazione digitale degli studenti e delle studentesse, per questo pianifica percorsi da mettere in pratica insieme per sensibilizzare i genitori sulle tematiche relative alle TIC.

Il regolamento scolastico e anche il "Patto di corresponsabilità" hanno specifici riferimenti alle tecnologie digitali e all'ePolicy.

A tale proposito è importante informare i genitori sulle condotte che si dovranno adottare a scuola e, in generale, offrire loro consigli da mettere in pratica con i propri figli.

Attraverso gli incontri formativi aperti alla famiglia, la scuola:

- fornisce ai genitori consigli sull'uso delle tecnologie digitali nella comunicazione scuola/ famiglie (es. mail, gruppo whatsapp, sito della scuola etc.)
- fornisce ai genitori consigli o linee guida sull'uso delle tecnologie digitali nella comunicazione con i figli e in generale in famiglia (ad es. a tal fine si consiglia di fare riferimento alla sezione dedicata ai genitori del sito www.generazioniconnesse.it accessibile anche dal sito web della scuola);
- organizza percorsi di sensibilizzazione e formazione dei genitori su un uso responsabile e costruttivo della Rete in famiglia e a scuola.
- prevede azioni e strategie per il coinvolgimento delle famiglie mediante l'organizzazione di iniziative in cui anche gli studenti e le studentesse siano protagonisti.
- offre un supporto costante alle famiglie sia in termini di strumentazione che di utilizzo tramite l'azione dell'animatore digitale, della funzione strumentale A2, dell'amministratore di Gsuite, e del tecnico di Ambito, per una agevole Scuola a Distanza.

Una particolare attenzione potrà essere dedicata a consigli, indicazioni e informazioni su iniziative e azioni della scuola, in riferimento ai rischi connessi ad un uso distorto della Rete da parte degli studenti e delle studentesse.

Ciò in continuità anche con l'art. 5 (comma 2) della legge 29 maggio 2017, n.71 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo" che prevede l'integrazione, oltre che del regolamento scolastico, anche del "Patto di Corresponsabilità", con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari "commisurate alla gravità degli atti compiuti", al fine di meglio regolamentare l'insieme dei provvedimenti sia di natura disciplinare che di natura educativa e di prevenzione al fenomeno.

Il nostro piano d'azioni

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

- 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 del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

personali.

L'Istituto Comprensivo Calimera si è adeguato al GDPR (General Data Protection Regulation), il Regolamento attraverso il quale la Commissione Europea intende rafforzare la protezione dei dati personali di cittadini dell'Unione Europea, entrato in vigore il 25 Maggio 2018.

È un obbligo delle pubbliche amministrazioni, rilasciare idonea informativa privacy fornita alle famiglie e a tutti i dipendenti, fornitori, stakeholders. Le informative sono pubblicate nella sezione privacy del sito della scuola ai seguenti link (https://www.icscalimera.edu.it/privacy-2/)

- https://www.icscalimera.edu.it/wp-content/uploads/2018/12/INFORMAZIONI-SUL-TRATTAMENTO-DEI-DATI-PERSONALI-signed-1.pdf
- https://www.icscalimera.edu.it/wp-content/uploads/2018/07/INFORMAZIONI-SUL-TRATTAMENTO-DEI-DATI-PERSONALI-signed-1.pdf

PERSONE AUTORIZZATE AL TRATTAMENTO

Consultare i seguenti link al sito della scuola, relativi agli atti di designazione

- https://www.icscalimera.edu.it/wp-content/uploads/2018/12/Atto-di-designazione-collaboratori-scolastici-_revGDPR-3.pdf
- https://www.icscalimera.edu.it/wp-content/uploads/2018/12/Atto-di-designazione-docenti_revGDPR-1-1.pdf
- https://www.icscalimera.edu.it/wp-content/uploads/2018/12/Atto-di-designazione-assistenti-amministrativi_revGDPR-2.pdf

A seguito del DPCM 4 MARZO 2020 si è resa necessaria l'attuazione di sistemi di formazione a distanza (FAD), che per la scuola vengono indicati con Didattica a Distanza. Al fine di garantire anche in situazioni di emergenza un corretto approccio al GDPR sul sito della scuola sono pubblicati anche i seguenti documenti:

- https://www.icscalimera.edu.it/wp-content/uploads/2020/04/Informativa-FAD-Scuola.pdf
- https://www.icscalimera.edu.it/wp-content/uploads/2020/04/Informativa-Telelavoro-Scuola.pdf

Con nota n. 388 del 17 marzo 2020 il MI ed il Garante della Privacy (Registro dei provvedimenti n. 64 del 26 marzo 2020) forniscono le prime istruzioni e disposizioni per garantire il rispetto della normativa sulla privacy nei trattamenti che le scuole hanno dovuto improvvisare in piena emergenza, per permettere lo svolgimento dell'attività amministrativa e didattica da remoto.

Anche in condizioni di emergenza continua a valere la normativa sulla privacy, che tutela un diritto fondamentale dell'individuo, il quale però non è assoluto e deve trovare un giusto bilanciamento con altri diritti fondamentali.

Tutte le liberatorie inerenti i dati personali relative al trattamento delle immagini (foto, video) sono inserite in apposita modulistica sul sito e nel diario personalizzato della scuola. https://www.icscalimera.edu.it/modulistica/

3.2 - Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.*
4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

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

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

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

Strumentazioni scolastiche per l'accesso ad internet
Il personale scolastico è tenuto a seguire le seguenti regole di accesso alle strumentazioni:

● È consentito l'uso delle strumentazioni scolastiche esclusivamente per uso didattico. Usi diversi da questo vanno autorizzati dal Dirigente Scolastico.

● Le strumentazioni scolastiche devono essere maneggiate con attenzione al fine di evitarne danni strutturali.

● Le strumentazioni, dopo essere state utilizzate, vanno riposte con cura e non separate dagli accessori d'uso (caricabatterie, mouse, custodia…).

● Il personale scolastico è tenuto a segnalare tempestivamente al responsabile della custodia delle strumentazioni la mancanza delle stesse o di eventuali accessori.

● Le strumentazioni vanno custodite nelle aule blindate della scuola (una per piano) o nei bauletti blindati se l'edificio è videosorvegliato.

● Il personale docente non è tenuto a creare nuovi utenti sulle strumentazioni scolastiche.

● È vietato installare software di uso non didattico.

Gli alunni sono tenuti a rispettare le seguenti regole d'accesso alle strumentazioni:

● È consentito l'uso delle strumentazioni scolastiche esclusivamente per uso didattico, secondo le disposizioni del docente presente.

● Le strumentazioni, dopo essere state utilizzate, vanno riposte con cura e non separate dagli accessori d'uso (caricabatterie, mouse, custodia…)

● Le strumentazioni scolastiche devono essere maneggiate con attenzione al fine di evitarne danni strutturali.

● Gli alunni possono accedere solo all'utente a loro riservato, libero da password.

● È consentito il salvataggio di documenti personali a scopo didattico, utilizzando cartelle specifiche per ciascuna classe.

Accesso ad internet

Il personale scolastico è tenuto a seguire le seguenti regole di accesso ad Internet:

● È possibile accedere ad internet attraverso strumentazioni in dotazione all'istituto o attraverso dispositivi personali.

● L'accesso ad internet e la navigazione attraverso le strumentazioni scolastiche è riservato ad un uso strettamente didattico.

● È possibile accedere ad account personali durante l'uso di internet, ma è obbligatorio il logout al termine.

● Non è consentito il salvataggio di dati personali (nomi utenti, account e password) nei browser delle strumentazioni scolastiche.

● È vietato scaricare o installare da internet materiale potenzialmente dannoso, di provenienza non sicura o non legale.

Gli alunni sono tenuti a rispettare le seguenti regole d'accesso ad internet:

● È vietato l'accesso ad internet senza autorizzazione da parte del personale docente.

● È vietata la navigazione in assenza del docente.

● L'accesso ad internet e la navigazione attraverso le strumentazioni scolastiche è riservato ad un uso strettamente didattico e nel rispetto di diritti della cittadinanza digitale e delle norme vigenti di utilizzo legale della rete.

● È vietato il salvataggio di dati personali (nomi utenti, account e password) nei browser delle strumentazioni scolastiche.

● È vietato scaricare da internet materiale senza l'autorizzazione del docente.

Tutti gli operatori presenti a qualsiasi titolo nella scuola (esperti esterni, collaboratori, ditte esterne…) e i genitori che accedono all'edificio scolastico, dovranno attenersi alle regole generali previste per il personale.

Gestione accessi - account

In seguito al progetto LAN/WLAN la scuola si è dotata di WILLO SCHOOL, un sistema di Hot Spot con captive portale per l'identificazione degli utenti naviganti, attivo nella sede centrale di via Ugo Foscolo. Qui sono presenti due reti separate: una riservata alla segreteria e una didattica. Le due reti non comunicano tra loro al fine di garantire la riservatezza dei dati di segreteria. I computer degli uffici amministrativi sono inoltre protetti da password.

Negli altri plessi è presente un modem-router che permette la messa in rete e la connessione ad internet dei dispositivi presenti nell'edificio. Per accedere alla rete è necessario che il dispositivo sia collegato tramite cavo o con Wi-Fi.

Per connettere un dispositivo al Wi-Fi scolastico è necessario inserire la chiave di sicurezza, custodita dall'Animatore Digitale, dai docenti del team digitale o dai responsabili di laboratorio. I docenti tutti avranno cura di tenerlo riservato.

- Accesso aula informatica con prenotazione
- Computer dedicato ad ogni classe collegato alla rispettiva LIM

- Nel laboratorio informatico i computer hanno unico accesso con reset automatico ad ogni riavvio, che ripristina le condizioni iniziali stabilite dall'amministratore garantendo azione di pulizia e antivirus

- Eventuale installazione di programmi o software è prevista solo previa autorizzazione dell'amministratore (Scuola Secondaria). Nei plessi della scuola primaria, il controllo viene effettuato dai responsabili dei laboratori

- Repository dei lavori solo nella cartella archivio presente sul server con collegamento su ogni singolo client
- Utilizzo account classe tramite card willo max 2h per eventuali lavori di classe con dispositivi

mobili, personali o della scuola (plesso Sec. Calimera)
- Annotazione su apposito registro di: - firme di presenza - verifica iniziale di attrezzature e rilevazione eventuali anomalie - verifica finale di attrezzature e rilevazione eventuali anomalie

- Password - Le password dei wifi, dove c'è Hot Spot, sono gestite dal personale scolastico attraverso l'utilizzo di card per classe della durata di 2 ore; sono comunicate agli alunni solo nelle attività BYOD e durante l'utilizzo dei laboratori informatici nei vari plessi

- Backup - Nell'area segreteria periodicamente vengono effettuati backup automatizzati su dispositivo di rete

- E-mail - Il personale scolastico, le famiglie, gli operatori esterni e gli Enti potranno comunicare con la segreteria inviando la posta ai due indirizzi a disposizione dell'Istituto:

leic816004@istruzione.it

PEC: leic816004@pec.istruzione.it
Attualmente gli indirizzi di posta elettronica dei genitori, dei docenti e del personale della scuola sono gestiti dalla segreteria, attraverso registro elettronico. La scuola può utilizzare una lista di indirizzi di utenti selezionati per distribuire del materiale, credenziali, comunicazioni. Gli indirizzi email non vanno divulgati. Cancellare il mittente o i vari destinatari quando si invia un messaggio a più destinatari che non si conoscono tra loro.

-- L'account email di Gsuite, sarà fruibile dagli utenti nell'anno scolastico 2020-2021. Tale account sarà utilizzato come strumento per la didattica a distanza.

L'amministratore genera le credenziali, obbligando il cambio password al primo accesso e le invia attraverso il registro elettronico alle famiglie. L'eventuale cambio password viene gestito dall'amministratore. L'account degli alunni non può ricevere e inoltrare mail al di fuori del dominio. Docenti e ATA invece hanno un account libero da restrizioni.

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.

Registro elettronico

Il registro elettronico on line è uno strumento al quale possono accedere tutti i membri della

Comunità Scolastica, previa registrazione da parte della segreteria.
L'IC di Calimera utilizza il Registro elettronico Argo Didup.
L'uso del registro è personale e riservato: ogni utente deve provvedere affinché i dati di login restino riservati e si impegna a cambiare password nel caso in cui la riservatezza degli stessi sia stata violata.

NORME PER GLI STUDENTI E PER I LORO GENITORI

CREDENZIALI DI ACCESSO

Le famiglie accedono al Registro Elettronico per la parte di propria competenza attraverso codici di accesso riservati (username e password) che vengono prodotti in forma riservata dal personale ATA incaricato, in numero pari alle mail indicate al momento dell'iscrizione (una sola mail=una sola password).

Le credenziali sono personali, riservate e non cedibili ad altre persone. Chi le riceve è responsabile del loro corretto utilizzo. Le credenziali assegnate a inizio del percorso scolastico non vengono modificate negli anni successivi.

In caso di smarrimento delle credenziali è possibile avviare la procedura di recupero in modo automatico. Qualora ciò risultasse impossibile, studenti e famiglie possono rivolgersi alla Segreteria Alunni.

COMUNICAZIONI SCUOLA-FAMIGLIA

La scuola comunica con la famiglia tramite le seguenti funzionalità del Registro Elettronico:
-NOTE DISCIPLINARI
-BACHECA DI CLASSE E BACHECA ALUNNI
-DOCUMENTI CONDIVISI
-E MAIL AI GENITORI

I genitori utilizzano il registro per:

- leggere le comunicazioni ufficiali della segreteria e dei docenti
- controllare quotidianamente il registro, in particolare le assenze, i voti, le note, i documenti di valutazione e l'agenda di classe, la bacheca. A tal proposito si fa presente che la rilevazione degli ingressi agli studenti avviene in avvio di prima ora di lezione, tranne in casi di disservizio temporaneo della linea. Nei casi di ingresso ritardato o di uscita anticipata, presenze ed assenze verranno segnalate sul registro dal docente in servizio nell'ora e saranno conteggiate ai fini della determinazione della validità dell'anno scolastico del singolo studente
- effettuare le prenotazioni dei colloqui con i docenti
- rispondere alle comunicazioni del personale docente
- comunicare alla segreteria eventuali incongruenze nei dati anagrafici personali o del proprio figlio.

NORME PER I DOCENTI

Tutti i docenti utilizzano il Registro Elettronico per:

- leggere le comunicazioni ufficiali della segreteria

- inserire la propria firma nell'ora corrente di lezione

- rilevare presenze e assenze degli studenti compresi ingressi in ritardo ed uscite anticipate. A tal proposito si fa presente che la verifica e la registrazione della giustificazione dell'assenza sono a cura del docente della prima ora. Il docente della seconda ora (o di ore successive) verifica e registra le giustificazioni degli alunni che entrano in ritardo

- inviare comunicazioni e avvisi ai genitori tramite l'apposita sezione

- comunicare a studenti e famiglie le valutazioni per la specifica materia (Scuola Secondaria)

- comunicare alla famiglia eventuali problematiche comportamentali e relazionali che emergono per lo specifico studente

- compilare le attività della lezione

- assegnare i compiti

- annotare significativi episodi della vita di classe da portare al CdC

- pubblicare e condividere con docenti e alunni materiale didattico rispettando le norme della privacy

- tenere periodicamente aggiornate le sezioni riguardanti la Programmazione e i voti
- compilare le proposte di voto e i documenti di valutazione entro i termini previsti per lo scrutinio
- comunicare alla segreteria eventuali incongruenze nell'elenco degli alunni
- segnalare all'Amministratore del registro eventuali anomalie nel funzionamento.

CREDENZIALI PERSONALI E FIRMA REGISTRI

E' vietato cedere, anche solo temporaneamente, il proprio codice utente e la propria password. L'utente intestatario verrà considerato responsabile di qualunque atto illecito perpetrato con quell'account.

Il recupero delle credenziale avviene in automatico, se nel proprio profilo il docente ha memorizzato un indirizzo di email valido.

Le credenziali di accesso di ogni docente rimangono attive fino alla permanenza del docente in servizio nell'Istituto.

Esse NON devono essere memorizzate in funzioni di login automatico, in un tasto funzionale o nel browser utilizzato per la navigazione internet o in computer di uso comune.

Per garantire la massima sicurezza, il docente è tenuto al cambio periodico della propria password.

La compilazione del registro elettronico spetta esclusivamente al docente presente in aula.

Per nessun motivo si possono delegare colleghi, alunni o altre persone a tale mansione.

La firma di presenza deve essere apposta giornalmente. In caso di particolari problemi tecnici, la firma dovrà essere regolarizzata il prima possibile.

Se la classe partecipa a visita d'istruzione o altra attività fuori aula, il controllo delle presenze spetta al docente accompagnatore che firmerà le ore di presenza della classe fuori aula.

Si rammenta che la firma sul registro di classe fa parte degli obblighi di servizio dei docenti.

Uffici amministrativi

Il Dirigente scolastico, il DSGA, il personale di segreteria e l'Amministratore del registro possono accedere a specifiche aree riservate, personalizzate secondo ruoli e mansioni stabilite, per configurare le impostazioni di sistema e inviare comunicazioni al personale.
Il Dirigente scolastico, quale supervisor ha accesso ad ogni area del registro.

Come per il personale docente, anche per il personale amministrativo è vietato cedere, anche solo temporaneamente, il proprio codice utente e la propria password. L'utente intestatario verrà considerato responsabile di qualunque atto illecito perpetrato con quell'account.

Il recupero delle credenziale avviene in automatico, se nel proprio account è stato memorizzato un indirizzo di email valido.

Le credenziali di accesso di ogni amministrativo rimangono attive fino alla permanenza in servizio nell'Istituto.

Esse NON devono essere memorizzate in funzioni di login automatico, in un tasto funzionale o nel browser utilizzato per la navigazione internet o in computer di uso comune.

Per garantire la massima sicurezza, il personale è tenuto al cambio periodico della propria password.

Per nessun motivo si possono delegare colleghi o altre persone alla compilazione del proprio registro.

La firma di presenza deve essere apposta giornalmente. In caso di particolari problemi tecnici, la firma dovrà essere regolarizzata il prima possibile.

GSUITE

Gsuite comprende: Gmail, Drive, Calendar, Documenti, Fogli, Presentazioni, Moduli, Hangouts Meet, Classroom.
L'Accesso nella suite è possibile solo con profilo istituzionale (@icscalimera.edu.it)
Con G Suite for Education gli insegnanti possono creare occasioni di apprendimento a distanza con strumenti efficaci combinati in modo interattivo in base alle esigenze e all'evoluzione della situazione didattica.

Google Meet e Classroom sono gli applicativi che abilitano direttamente la didattica a distanza.

Meet consente di comunicare via chat e videoconferenza, sia in bilaterale che in gruppo. Classroom consente di gestire classi virtuali, distribuire compiti e test, dare e ricevere commenti su un'unica piattaforma.

Gmail: offre il servizio email di Google.

Documenti, Fogli, Presentazioni: consentono a studenti e insegnanti di creare, leggere e modificare documenti in tempo reale.

Drive è il sistema per archiviare qualsiasi file in modo sicuro e illimitato. Insegnanti e studenti possono condividere i file in modo rapido, invitando altre persone a visualizzare, commentare e modificare qualsiasi file o cartella. L'autore mantiene il controllo del documento e può gestirne l'accesso in qualunque momento.

Moduli permette di effettuare verifiche, test, sondaggi o creare rapidamente un elenco di presenze o turni.

Calendar permette di creare appuntamenti, promemoria, elenchi di attività da svolgere.

I servizi principali di G Suite non contengono annunci né utilizzano le informazioni ottenute per finalità pubblicitarie. Non solo, tutti i servizi principali di G Suite for Education sono conformi alle norme COPPA (Child's Online Privacy Protection Act) e FERPA (Family Educational Rights and Privacy Acts).

La classroom di Gsuite sarà utilizzata dai ragazzi per la didattica a distanza e per attività programmate dai docenti.
I docenti utilizzano classroom anche per gli incontri di formazione, di progettazione e riunioni collegiali.
Gli alunni utilizzano la classroom di Gsuite sia per le videolezioni sincrone attraverso meet **attivabile solo da classroom** sia come classe virtuale e piattaforma didattica DaD (dal prossimo anno scolastico).

Regole di utilizzo

a) L'utente può accedere direttamente al suo account istituzionale collegandosi a Google.it, inserendo il suo nome utente: nome.cognome@icscalimera.edu.it
b) Gli account fanno parte del dominio icscalimera.edu.it di cui l'Istituto è proprietario
c) La password fornita inizialmente dall'Amministratore dovrà essere modificata al primo accesso
d) Nel caso di smarrimento della password, l'utente dovrà comunicare immediatamente l'accaduto all'Amministratore per il rilascio di una nuova password momentanea da cambiare al primo nuovo accesso
e) Ogni account è associato ad una persona fisica ed è perciò strettamente confidenziale
f) Le credenziali di accesso non possono, per nessun motivo, essere comunicate ad altre persone che non ne abbiano titolo né cedute a terzi
g) Le credenziali di accesso non possono essere altresì memorizzate all'interno dei browser installati nei dispositivi della scuola

h) L'utente è riconosciuto quale autore dei messaggi inviati dal suo account e quale ricevente dei messaggi spediti al suo account
i) L'account va usato esclusivamente per le finalità della scuola e per motivi strettamente collegati alle attività istituzionali che dipendono dal ruolo rivestito all'interno dell'Istituto (docenti, studenti)
j) Il servizio non va utilizzato per effettuare azioni e/o comunicazioni che arrechino danni o turbative alla rete o a terzi utenti o che violino le leggi ed i regolamenti vigenti
k) L'utente è responsabile delle azioni compiute tramite il suo account e pertanto esonera l'Istituto da ogni pretesa o azione che dovesse essere rivolta all'Istituto medesimo da qualunque soggetto, in conseguenza di un uso improprio.

Regole per le video lezioni

Un'apposita nota pubblicata sul sito della scuola nella sezione individuata dal banner DaD (https://www.icscalimera.edu.it/wp-content/uploads/2020/03/Didattica-a-Distanza-ICS.pdf) dà istruzioni operative sui corretti comportamenti da tenere usando le piattaforme web durante le video lezioni:

1. durante lo svolgimento delle lezioni online occorre mantenere un comportamento serio e responsabile analogo a quello che viene adoperato a scuola

2. è vietato consentire l'accesso alle piattaforme a soggetti non autorizzati

3. la chat dovrà essere usata solo per finalità didattiche

4. tutti i materiali utilizzati sono ad esclusivo uso didattico e riservati.

Utilizzo del microfono

1. Durante la video-lezione occorre disattivare il microfono

2. L'attivazione del microfono deve avvenire solo previa autorizzazione del docente.

Registrazioni audio/video

1. L'acquisizione e divulgazione di registrazioni audio/video e di immagini, acquisite nel corso della video lezione, sono severamente vietate /o consentite solo per uso didattico

2. L'utilizzo non autorizzato di immagini o video delle lezioni online espongono l'alunno a sanzioni sotto il profilo disciplinare, civile e/o penale, secondo la normativa vigente.

Messaggistica Gsuite - Stream di classroom Gsuite – Chat Gsuite
La nostra scuola utilizza anche come strumenti di comunicazione on line lo stream di classroom di Gsuite.

Regole di utilizzo per docenti e studenti

- 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
- 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, rispettando sempre le regole della privacy
- 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 esaustivi allo stesso tempo
- L'insegnante è il moderatore dei mezzi di comunicazione, dei gruppi di discussione e delle chat-rooms, impiegati a scopo didattico a scuola - Sono permesse solo chat a scopi didattici e comunque sempre con la supervisione dell'insegnante per garantire la sicurezza.

Blog e sito web della scuola

Il sito web dell'istituto si pone come strumento di comunicazione di contenuti educativi e di attività didattiche

- L'istituto ne gestisce le pagine e garantisce che i contenuti siano accurati e appropriati

- Detiene inoltre i diritti d'autore dei documenti prodotti in proprio o dei quali è stato chiesto e ottenuto il permesso all'autore

- Nel caso di sponsorizzazioni esterne si farà ricorso a ringraziamenti pubblici

- Nella pubblicazione di immagini degli alunni è richiesta la liberatoria da parte dei genitori

- Il sito dispone di un'area pubblica e di un'area riservata ai docenti con accesso previo login

- I docenti dispongono anche di una password interna per consultare o scaricare modulistica e documenti appositamente crittografati

- I lavori prodotti dagli alunni, ai quali è destinata una specifica area del sito, sono soggetti al controllo degli amministratori che ne possono bloccare la pubblicazione se non conformi alle norme di sicurezza vigenti

Social network della scuola: Canale You tube - Pagina facebook d'Istituto

- All'interno dei social network evitare di condividere dati personali e di contatto, come numeri di telefono o indirizzi

- Evitare di scambiare file con utenti sconosciuti e verificare sempre l'origine dei file effettuando un controllo con un antivirus aggiornato

- Se durante una chat, un forum o in una qualsiasi discussione online, l'interlocutore diviene volgare, offensivo o minaccioso, segnalare al docente e abbandonare la conversazione

- Quando si riscontra un comportamento riconducibile ad un illecito, segnalarlo

- Evitare di scaricare dei file illegali o protetti dal diritto d'autore

- I sistemi di messaggistica dei Social Network hanno le stesse regole della posta elettronica quindi è necessario preservare la privacy di tutti, cancellando il mittente o i vari destinatari quando si invia un messaggio a più destinatari che non si conoscono tra loro

- Evitare di inoltrare spam e di perpetrare qualunque tipo di abuso usando i messaggi elettronici

- Quando si scambiano contenuti multimediali o si pubblicano video con colonna sonora o musica di sottofondo bisogna essere sicuri di averne il diritto d'uso (CC) e di non utilizzare alcun file coperto da copyright; la scuola, essendo ad indirizzo musicale, produce e utilizza a questo scopo testi musicali inediti dei quali detiene il diritto d'autore

- I contenuti pubblicati sulle applicazioni web dei social network, hanno diversi livelli di visibilità, per esempio singoli utenti o tutti gli utenti della rete, che devono sempre essere tenuti a mente, dando a ciascun contributo i corretti livelli di privacy: pertanto, quando si inizia a pubblicare materiale in una community bisogna studiare ed imparare ad utilizzare correttamente le funzioni per l'impostazione dei livelli di privacy

- Dal momento che ciò che viene pubblicato su un social network è persistente e spesso non è facile da cancellare, bisogna evitare di contribuire con materiale che in futuro non si vorrebbe veder pubblicato

- Quando si contribuisce con del materiale in un ambiente condiviso, l'utente è tenuto ad essere coerente con il contesto e le regole di fatto della community, evitando di pubblicare materiale inadeguato e che potrebbe risultare fuori contesto: ci sono momenti e luoghi virtuali per parlare di qualsiasi tema nel rispetto dei propri interlocutori

- Quando si fa uso di etichette per catalogare un contenuto/utente (tag), bisogna assicurarsi che sia coerente con il contenuto o che indichi la persona corretta; quando il tag riguarda una persona, contattarla preventivamente per ottenere il consenso a collegare l'identità della persona al contenuto

- Aggiungere alla propria rete di amici solo le persone che hanno in vari modi dimostrato di essere affidabili, con cui si è a proprio agio e di cui siamo a conoscenza della reale identità

- Se si instaura un'amicizia virtuale con persone di cui non si conosce la reale identità, evitare di condividere contatti e dati personali e contenuti privati, soprattutto se riguardano terze persone

- Tenere sempre a mente che gli "amici degli amici" o di componenti del proprio "network" sono molti e spesso hanno modo, nonostante siano sconosciuti, di avere accesso alle informazioni e ai contenuti personali

- Se si ha accesso alle comunicazioni private di altri utenti, ad esempio perché l'utente ha impostato

in maniera sbagliata i livelli di privacy, bisogna notificarlo all'utente ed evitare di leggere i messaggi privati

- La reputazione digitale è persistente e si diffonde velocemente, pertanto, non bisogna mai diffamare altre persone, soprattutto se le stesse non sono presenti sul social network e non possono accorgersi del danno subito.

Gruppi whatsapp

All'inizio dell'anno scolastico è preoccupazione dei genitori creare un gruppo whatsapp di classe tenersi aggiornati sulla vita di classe. Si ricorda la funzione dei Gruppi WhatsApp dei genitori di una classe: permettere di scambiarsi, in maniera immediata, informazioni utili su ciò che riguarda la scuola e, per l'esattezza, sulla classe dei figli.

Si raccomanda un utilizzo consapevole e appropriato secondo le regole del rispetto della privacy:

- mantenere sempre la cosiddetta "netiquette", cioè le regole (non scritte) del galateo web

- evitare di condividere contenuti inappropriati, a partire dalle bufale (controllare sempre le fonti) oppure foto o messaggi di altri senza il consenso dei genitori

- non utilizzare il gruppo per messaggi rivolti solo a un numero limitato di genitori

- Il rappresentante di classe o chi per lui, deve svolgere l'importante funzione di moderatore del gruppo, invitando al rispetto delle regole del gruppo.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/lle studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

La presente ***ePolicy*** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

Per gli studenti:

Non è consentito l'uso di dispositivi personali (notebook, tablet, cellulare, ecc …), fatta eccezione per gli alunni con DSA o disabili per i quali ci sia evidenza di averne necessità per un uso strettamente didattico o per la comunicazione, in questo caso i genitori dovranno farne richiesta scritta documentata al Dirigente. Viceversa, i team o i consigli di classe potranno promuovere, per gli alunni per i quali ci sia evidenza, che l'uso di dispositivi personali possa migliorare il percorso didattico e rimuovere ostacoli all'apprendimento, con la condivisione delle famiglie, l'uso di device personali.
Telefono: l'utilizzo per motivi personali dei telefoni dell' Istituto è vietato, salvo gravi motivi.
Telefoni cellulari: i telefoni cellulari degli alunni devono essere spenti all'ingresso della scuola e custoditi all'interno di borse/zaini. Non è pertanto consentito il loro utilizzo in alcun modo nel periodo di permanenza all'interno della scuola. (CM 362 del 25/08/98 e Direttiva n.30 del 2007). Le famiglie che ritenessero, per soggettive motivazioni, di dare comunque in uso ai propri figli il telefono cellulare, sono tenute a far rispettare quanto indicato nel Regolamento. Si ricorda che genitori/alunni possono utilizzare per comunicazioni urgenti le linee telefoniche dell'Istituto. Durante le uscite didattiche il telefono cellulare potrà essere autorizzato solo nei momenti consentiti dai docenti.
Gli alunni che dovessero contravvenire alle sopraindicate regole potranno incorrere in provvedimenti disciplinari, secondo le norme previste dal Regolamento di disciplina (Cap. IX)
L'Istituto non sarà comunque ritenuto responsabile in caso di furto o danneggiamento accidentale.

Inoltre, si rammenta che nell'edificio scolastico e nell'area di pertinenza, è vietato registrare foto, video e audio con dispositivi digitali personali se non con l'autorizzazione dei docenti e per attività programmate.

Le foto e i video eventualmente registrati in queste occasioni, dietro autorizzazione dei docenti, dovranno avere un uso personale e non potranno essere diffusi in rete qualora siano state riprese terze persone (altri alunni, genitori, docenti ed operatori).

Per i docenti

È consentito l'uso di strumentazioni personali (notebook, tablet…) per attività didattiche o extracurricolari, ma l'Istituto non sarà ritenuto responsabile in caso di furto o danneggiamento accidentale.

L'uso di internet per fini personali, attraverso dispositivi privati, non è consentito durante l'orario di servizio; è invece consentito al di fuori dell'orario di servizio, nel rispetto dei diritti della cittadinanza digitale e delle norme vigenti di utilizzo legale della rete.

Non è, comunque, consentito l'acceso ad internet attraverso la rete scolastica per fini personali.

Non è consentito l'uso del cellulare durante l'orario di servizio se non per attività didattiche.

In caso di viaggi d'istruzione, recite, progetti sul territorio ed altre situazioni affini, i docenti accompagnatori possono utilizzare dispositivi digitali personali per effettuare foto e video che non

potranno comunque essere pubblicati in rete attraverso social network o siti internet.

Personale amministrativo e i collaboratori scolastici

Per garantire la sicurezza dei dati sensibili, non è consentito svolgere attività amministrativa su dispositivi informatici personali (notebook, tablet...).

Non è, comunque, consentito l'acceso ad internet attraverso la rete scolastica per fini personali.

Non è, inoltre, consentito l'uso del cellulare per fini personali durante l'orario di servizio.

Altri operatori

Tutti gli altri operatori presenti a qualsiasi titolo nella scuola (esperti esterni, collaboratori, ditte esterne...) dovranno attenersi alle norme previste per il personale scolastico.
Telefono: l'utilizzo per motivi personali dei telefoni dell' Istituto è vietato, salvo gravi motivi.
Telefoni cellulari: i telefoni cellulari dei docenti devono essere spenti o tenuti in modalità silenziosa all'ingresso della scuola e custoditi all'interno di borse/zaini. Non è pertanto consentito il loro utilizzo nel periodo di permanenza all'interno della scuola, se non per gravi motivi e/o mal funzionamento del telefono di Istituto.
Per il personale della scuola
Telefono: l'utilizzo per motivi personali dei telefoni dell' Istituto è vietato, salvo gravi motivi (cfr Regolamento d'Istituto, sezione 7 "Spazi e attrezzature" Uso dei mezzi di comunicazione Telefono. Art. 33) cfr Regolamento di Disciplina, sezione 9: Regolamento di disciplina (artt. 41 – 46) (http://www.icscalimera.gov.it/regolamento-di-istituto/ 12)
Telefoni cellulari: i telefoni cellulari del personale della scuola devono essere spenti o tenuti in modalità silenziosa all'ingresso della scuola e custoditi all'interno di borse/zaini. Non è pertanto consentito il loro utilizzo nel periodo di permanenza all'interno della scuola, se non per gravi motivi e/o mal funzionamento del telefono di Istituto.

Il nostro piano d'azioni

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

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

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

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

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

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

Azioni di sensibilizzazione:

La nostra scuola da anni aderisce al progetto Generazioni Connesse e adotta le seguenti, come azioni consolidate:
- Coinvolgimento della comunità scolastica: momenti formativi aperti alle famiglie attraverso corsi, dibattiti, incontri, riguardo i rischi online che rappresentano tutte quelle situazioni problematiche derivanti da un uso non consapevole e non responsabile delle tecnologie digitali da parte di bambini/e, ragazzi e ragazze: adescamento online, cyberbullismo, sexting, violazione della privacy, pornografia (recenti ricerche hanno sottolineato come la maggior parte degli adolescenti reperisca

in Rete informazioni inerenti la sessualità, col rischio, spesso effettivo, del diffondersi di informazioni scorrette e/o l'avvalorarsi di falsi miti), pedopornografia (con questo termine si intende qualsiasi foto o video di natura sessuale che ritrae persone minorenni), gioco d'azzardo o gambling, internet addiction, videogiochi online (alcuni rischi associati possono essere ad esempio: contatti impropri con adulti, contenuti violenti e/o inadeguati; acquisti incontrollati, etc.), esposizione a contenuti dannosi o inadeguati (es. contenuti razzisti, che inneggiano al suicidio, che promuovono comportamenti alimentari scorretti, etc.), etc.

Durante gli interventi vengono fornite non solo le informazioni necessarie (utili a conoscere il fenomeno) ma anche le possibili soluzioni o i comportamenti da adottare, tramite brochure riassuntive dei contenuti trattati e vademecum specifici elaborati dagli esperti come suggerimenti di buone pratiche di prevenzione.

- Promozione della conoscenza dell'ePolicy nella comunità scolastica all'inizio dell'anno scolastico, in occasione degli open day per le iscrizioni al nuovo ordine di scuola, in occasione del Safer Internet Day.

- Pubblicizzazione del Patto educativo di corresponsabilità, delle "10 regole per giovani naviganti" e delle "10 dritte per navigare a vele spiegate" (dai kit didattici di Generazioni Connesse) e riferimenti al regolamento d'Istituto sul diario Smarty adottato dall'IC.

Azioni di prevenzione

- Implementazione del Curricolo verticale digitale con un insieme di attività, azioni ed interventi 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

- Promozione della cittadinanza digitale attraverso le esperienze formative legati ai vari progetti PTOF e PON di Cittadinanza digitale che permettono ai corsisti di conseguire la certificazione europea ECDL IT SECURITY

- Azione #15 PNSD scenari innovativi per lo sviluppo di competenze digitali applicate : USO SICURO DI INTERNET

-Giornata del Safer Internet Day

-Pagina sul sito della scuola dedicata al progetto Generazioni Connesse fruibile da docenti e studenti per un approccio attivo al materiale di supporto e alle buone pratiche già attivate nella scuola (https://www.icscalimera.edu.it/progetto-generazioni-connesse/)

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).

Con il termine cyberbullismo si intende una forma di prevaricazione mirata a danneggiare una persona o un gruppo, ripetuta e attuata attraverso l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC). Gli studiosi italiani condividono la definizione internazionale che vede il bullismo come un'oppressione, psicologica o fisica, reiterata nel tempo, perpetrata da una persona o da un gruppo di persone "più potenti" nei confronti di un'altra persona percepita come "più debole". Le caratteristiche di questa condotta sono: l'intenzionalità, la persistenza nel tempo, l'asimmetria relazionale e la natura sociale del fenomeno. Un prerequisito fondamentale per l'identificazione di tale problematica è la percezione da parte del soggetto vittima dello stesso di una forma di abuso da parte di terzi, questo per distinguere il bullismo da una situazione di conflitto.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a

questa problematica.

- Progetti di prevenzione e di contrasto al fenomeno

- Sportello di ascolto o focus group per alunni e famiglie

- Utilizzo di metodologia inclusiva come il circle time

- Aggiornamento del Regolamento d'istituto prevedendo apposite norme di cyberbullismo e navigazione online sicura

- Creazione di un team docenti con la partecipazione di un gruppo di alunni responsabile di attività di prevenzione

- Collaborazioni con partner esterni alla scuola (Forze dell'ordine, cooperative, associazioni...)

- Somministrazione di questionari agli studenti e ai genitori finalizzati al monitoraggio, anche attraverso il sito web della scuola

- Percorsi di formazione tenuti da esperti rivolti ai docenti e ai genitori (educatori e formatori) e dal referente sul Bullismo e Cyberbullismo sulla Legge 29 maggio 2017, n.71 disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo

- Ideazione e realizzazione di campagne pubblicitarie attraverso messaggi video e locandine informative

- Creazione sul sito web della scuola di una sezione dedicata, all'interno della pagina dedicata a Generazioni connesse e banner di richiamo nella Home page (es. Nodo blu)

- Formazione del personale scolastico e, in particolare, dei collaboratori scolastici al fine di una tempestiva segnalazioni di eventuali casi

- Comunicazione agli studenti e alle loro famiglie sulle sanzioni previste dal Regolamento di Istituto nei casi di bullismo, cyberbullismo e navigazione online a rischio

- Incontri educativi nelle classi che partecipano al progetto Generazioni Connesse e in ingresso nelle classi della secondaria, con esperti o con alunni più grandi che abbiano fatto la formazione "Generazioni Connesse" o la formazione IT Security

- Partecipazione annuale alla giornata del Safer Internet Day per le classi quarte e quinte della Scuola Primaria e per tutte le classi della Scuola Secondaria.

- La cassetta della denuncia anonima di comportamenti a rischio tra studenti

- Sondaggio anonimo sulle prepotenze a scuola

4.3 - Hate speech: che cos'è e come prevenirlo

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

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

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

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

Con il termine "Hate speech" si intende 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. A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica:

- Utilizzo di metodologia inclusiva

- Formazione interna e autoformazione del team docenti per l'innovazione e successiva formazione nelle classi come attività di prevenzione

- Percorsi di formazione tenuti da esperti rivolti ai docenti e ai genitori

- Ideazione e realizzazione di campagne pubblicitarie attraverso messaggi video e locandine informative

- Integrazione della pagina sulle STEM già presente sul sito della scuola di contenuti dedicati (https://www.icscalimera.edu.it/STEM/)

- Formazione del personale scolastico e, in particolare, dei collaboratori scolastici al fine di una tempestiva segnalazioni di eventuali casi

- Comunicazione agli studenti e alle loro famiglie sulle sanzioni previste dal Regolamento di Istituto nei casi di hate speech

- Incontri educativi nelle classi che partecipano al progetto Generazioni Connesse e in ingresso nelle classi della secondaria, con esperti o con alunni più grandi che abbiano fatto la formazione "Generazioni Connesse" o la formazione ITSecurity

- Partecipazione annuale alla giornata del Safer Internet Day per le classi quarte e quinte della Scuola Primaria e per tutte le classi della Scuola Secondaria

- Partecipazione ad eventuali progetti proposti dalla Direzione Generale per lo studente l'integrazione e la partecipazione "Noi siamo pari" del MIUR, proposti dall' Ambito o con partner diversi sulla prevenzione delle discriminazioni (es. il progetto "Il Melograno" sulla discriminazione di genere).

4.4 - Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

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

La nostra scuola è molto attenta al benessere digitale degli allievi. Ogni anno, in occasione del Safer Internet Day propone un piccolo sondaggio, a cura delle classi coinvolte nel progetto Generazioni Connesse su quanto tempo passano in internet i ragazzi e su cosa verte soprattutto la loro attenzione. Da questi sondaggi emergono le "mode" virtuali (Fortnite, Tik Tok, …) che generano nei ragazzi dipendenza da Internet, collegata all'uso di social o di videogiochi on line. Su questi dati si interviene strutturando gli interventi di sensibilizzazione e di prevenzione tramite il Safer Internet Day che, in questo modo, ogni anno hanno un taglio vicino alle esigenze dei ragazzi/e.
All'interno del gruppo classe, in sinergia con il Dirigente Scolastico, con eventuali esperti e con il consenso dei genitori, vengono strutturate regole condivise e vengono stipulati con loro "patti" d'aula per non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli studenti e delle studentesse, stabilendo chiare e semplici regole di utilizzo. Si cerca, inoltre, di proporre delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d'aula ad esempio adoperando la LIM o il dispositivo personale(BYOD) in modalità gioco al servizio dell'apprendimento.

4.5 - Sexting

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

La nostra scuola per sensibilizzare i ragazzi e le ragazze a questa tematica utilizza i kit didattici di Generazioni Connesse, i Super Errori e i laboratori annessi.
La scuola tuttavia applica i regolamenti per evitare l’utilizzo improprio dei dispositivi personali in orario scolastico.

4.6 - Adescamento online

Il ***grooming*** (dall’inglese “groom” - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di ***teen dating*** (siti di incontri per adolescenti). Un’eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

In Italia l’adescamento si configura come reato dal 2012 (art. 609-undecies – l’adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell’adescamento.

Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all’affettività e alla sessualità. Ciò aiuterebbe a renderli più sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri.
Per far questo la nostra scuola interviene attivando laboratori con i kit di Generazioni Connesse per prevenire ed affrontare la delicata problematica dell’adescamento. Attraverso la tecnica dello storytelling legata alla lettura di libri per ragazzi di cittadinanza digitale, vengono trattati tali rischi

e trasformati in fumetti, disegni, ministorie digitali, anche attraverso il coding. Questo sviluppa capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è). Nelle azioni di sensibilizzazione si utilizza la fonte "Schema sulle fasi dell'adescamento on line dei minori" a cura della Polizia Postale e delle Comunicazioni, all'interno del progetto "Una vita da social". Insieme all'Osservatorio Nazionale Adolescenza: https://www.adoleScienza.it/ per far prendere coscienza ai ragazzi/e di come l'adescamento on line passi attraverso varie fasi: dall'amicizia alla solidificazione del rapporto, valutazione del rischio, esclusività del rapporto, fase sessuale. Nella scuola Secondaria, seconde e terze classi, si propongono anche i percorsi con i video interattivi di Generazioni Connesse sull'adescamento on line, portando i ragazzi e le ragazze a scegliere tra le soluzioni proposte su come vorrebbero si concludesse la storia dei video.

4.7 - Pedopornografia

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

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

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

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

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

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

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

Il pericolo di imbattersi in rete in contenuti dannosi per il benessere emotivo dei nostri giovani studenti è molto elevato, pertanto la scuola, da un punto di vista strumentale, dota i dispositivi di software-filtro firewall inclusi nel servizio rete Willo e server DNS filtrati che impediscono l'accesso a siti dal contenuto nocivo.

In caso di rilevazione: si attiva il coinvolgimento della classe, la formazione con i kit didattici di Generazioni Connesse e/o l'approfondimento con esperti e, l'eventuale informazione sulle norme giuridiche apposite.

Il nostro piano d'azioni

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

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

☐ 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.

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.

☐ 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.

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

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

La scuola, come istituzione formativa ed educativa, ha il compito morale di fornire strumenti adeguati per il discernimento, responsabile e critico, dei vari aspetti della rete.

Il docente di classe, poiché trascorre diverse ore con i propri alunni, di solito è colui che potrebbe

accorgersi per primo di comportamenti riconducibili a un disagio.

Per questo potrà segnalare e tenere nota di situazioni particolari, mediante il Diario di bordo (Allegato A). Ulteriore strumento di indagine potrebbe rivelarsi l'agile sondaggio, elaborato dal referente per il bullismo e il cyberbullismo e dal gruppo di lavoro di Generazioni Connesse, per rilevare episodi di bullismo e cyberbullismo tra i ragazzi (Allegato B).

La scuola si impegna a segnalare fenomeni di:

-Cyberbullismo

-Sexting

-Adescamento o growing

5.2. - Come segnalare: quali strumenti e a chi

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

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

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

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

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

Strumenti a disposizione di studenti/esse

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

messi a loro disposizione:

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

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

COME SEGNALARE: QUALI STRUMENTI E A CHI	COME GESTIRE LE SEGNALAZIONI
Cyberbullismo - Comunicazione immediata di comportamenti legati al cyberbullismo, anche non verbali, a tutti i soggetti coinvolti (Collegio dei docenti, Consiglio d'istituto, famiglie) attraverso convocazioni adeguate Per i casi più gravi segnalazione alla polizia postale - Compilazione del diario di bordo - Help line del progetto "Generazioni Connesse" al numero gratuito 1.96.96 - Richiesta di sostegno ai servizi sociali o ad altre autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola)	Provvedimenti secondo il Regolamento di Istituto

Sexting In caso di rilevazione: - Coinvolgimento della classe e/o approfondimento con esperti - Informazione sulle norme giuridiche apposite - Compilazione del diario di bordo Per i casi più gravi segnalazione alla Polizia Postale - Help line del progetto "Generazioni Connesse" al numero gratuito 1.96.96 - Richiesta di sostegno ai servizi sociali o ad altre autorità competenti (soprattutto se il Sexting non si limita alla scuola) - Griglia di rilevazione con indicatori specifici utili a comprendere il fenomeno	- Segnalazione al Dirigente Scolastico - Consigli di classe - Segnalazione al referente della e-safety - Per casi gravi comunicazione scuola-famiglia - Collegio docenti - Consiglio d'Istituto - Intervento dell' Organo di Garanzia
Adescamento o Growing Per i contenuti online: - Segnalazione tramite sito "Generazioni Connesse" - Coinvolgimento obbligatorio dei genitori - Segnalazione al referente per l'e-safety - Segnalazione al Consiglio di classe - Comunicazione scuola-famiglia -Collegio docenti -Consiglio d'Istituto -Intervento dell' Organo di Garanzia	- Segnalazione al Dirigente Scolastico - Consigli di classe - Segnalazione al referente della e-safety Per casi gravi comunicazione scuola-famiglia - Collegio docenti - Consiglio d'Istituto

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.

Il nostro Istituto prevede:
- Segnalazione alla Polizia Postale

- Servizio Help line gestito da Telefono Azzurro nell'ambito del progetto Generazioni Connesse al numero gratuito 1.96.96, una piattaforma integrata che si avvale di telefono, chat, sms, whatsapp e skype, strumenti per aiutare i ragazzi e le ragazze a comunicare il proprio disagio alla Hotline "Stop-It" di Save the Children, all'indirizzo www.stop-it.it

- Servizio 114 Emergenza Infanzia. Servizio del Dipartimento per le Politiche della Famiglia-Presidenza del Consiglio dei Ministri. Il 114 Emergenza Infanzia è un servizio di emergenza rivolto a tutti coloro vogliano segnalare una situazione di pericolo e di emergenza in cui sono coinvolti

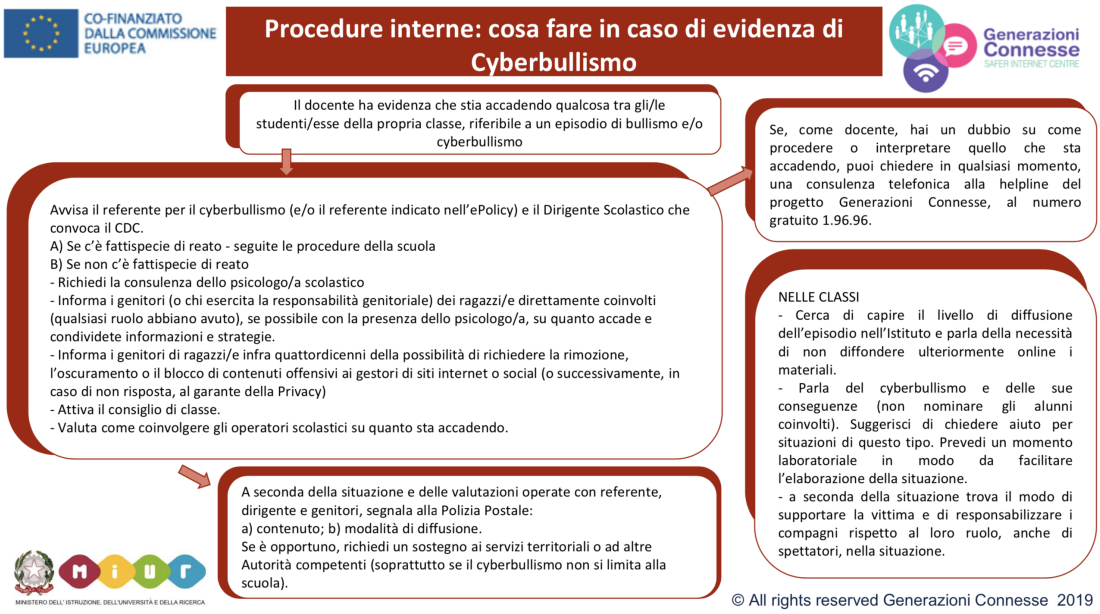
bambini e adolescenti

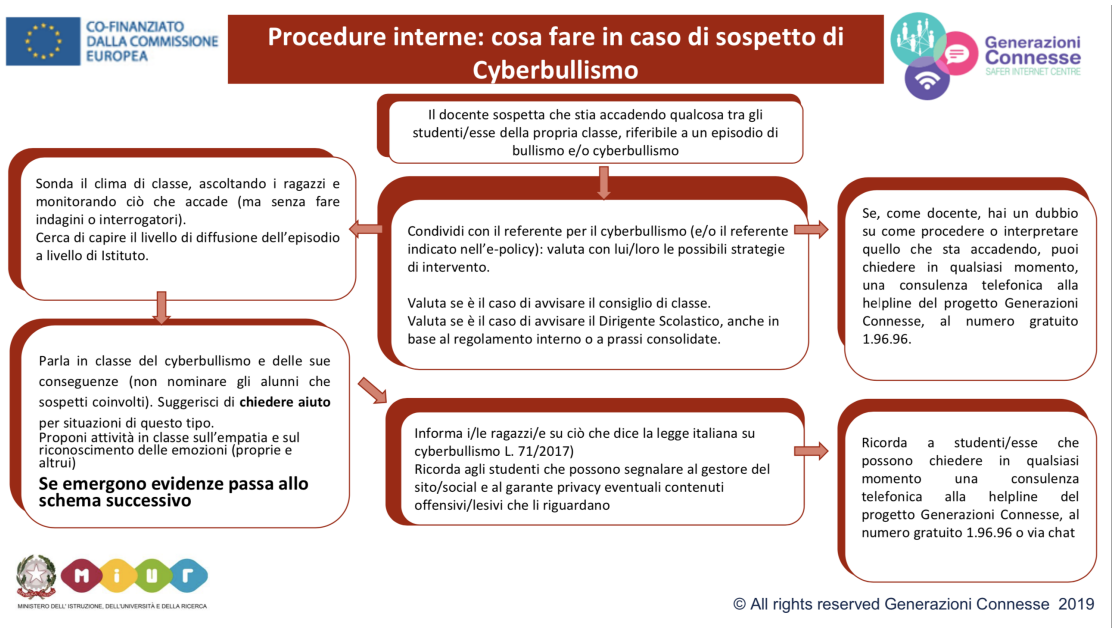
- Richiesta di sostegno ai servizi sociali o ad altre autorità competenti (soprattutto se il fenomeno non si limita alla scuola)

- AZIENDA SANITARIA LOCALE: Competenze/Servizi / Per avere un sostegno psicologico, psichiatrico o neuropsichiatrico sulle problematiche psicologiche, anche associate all'uso di Internet.

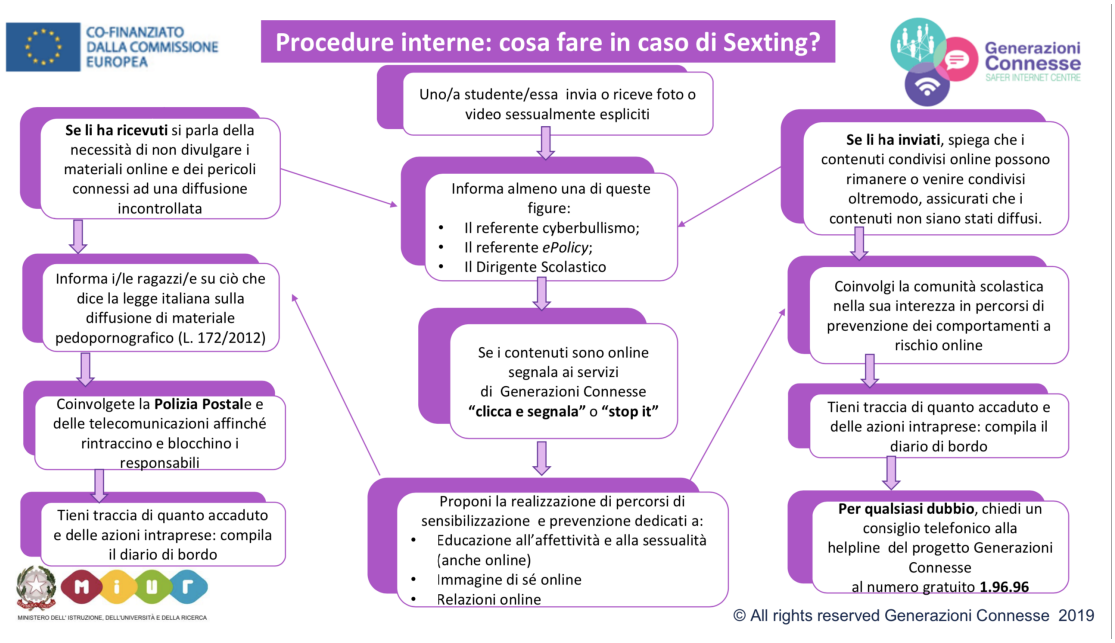
5.4. - Allegati con le procedure

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

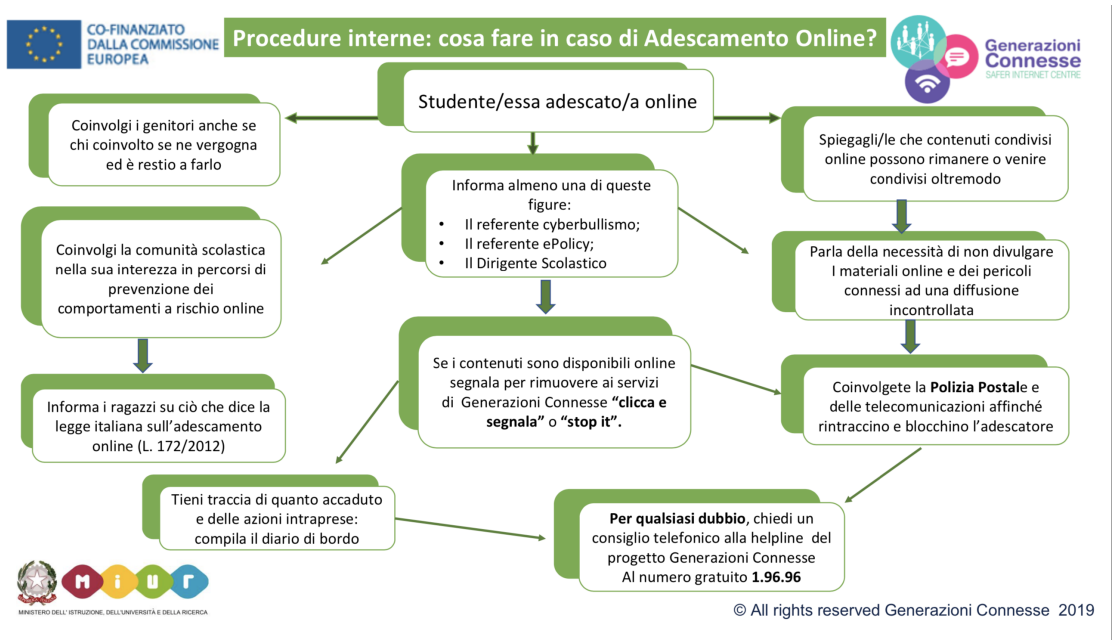




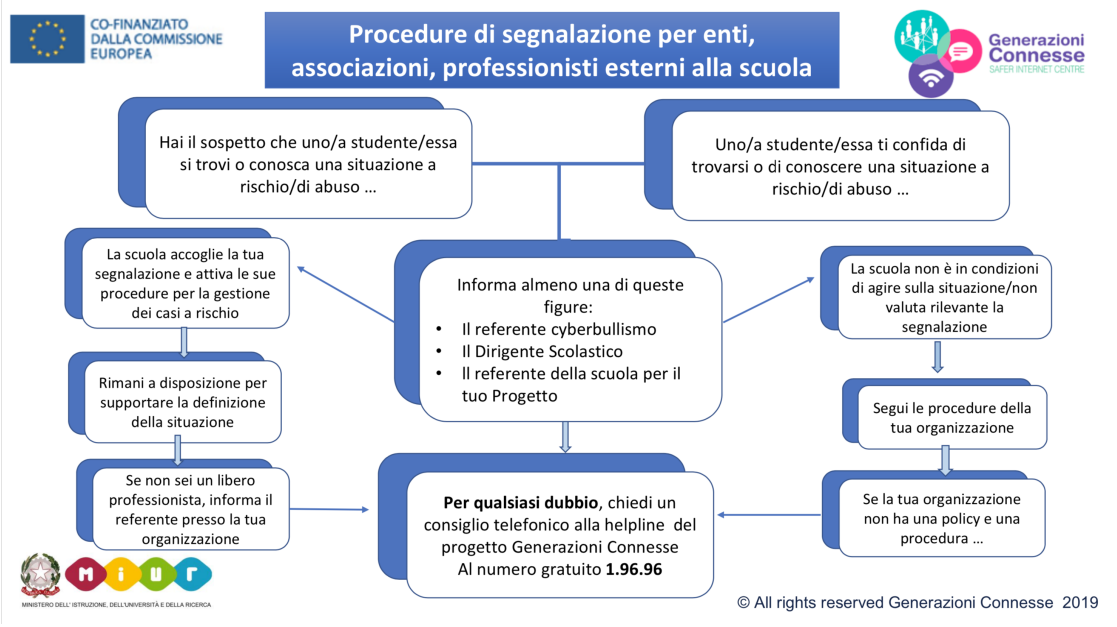
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

- Scheda di segnalazione

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

Procedure operative per la gestione delle infrazioni alla Policy

- Applicazione delle SANZIONI E AZIONI DI RESPONSABILIZZAZIONE previste dal Regolamento di disciplina http://www.icscalimera.gov.it/sezione-9-regolamento-di-disciplina/

- Applicazione del Regolamento privacy del Regolamento d'Istituto https://www.icscalimera.edu.it/privacy-2/

- Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni: schede segnalazioni strumenti: "Generazioni Connesse"

- Procedure operative per la gestione dei casi: schede diario di bordo "Generazione Connesse"

- Collaborazioni con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi.

Il nostro piano d'azioni

CASI	SANZIONI E AZIONI DI RESPONSABILIZZAZIONE
AZIONI DA INTRAPRENDERE A SECONDA DELLA SPECIFICA DEL CASO	1.Richiamo verbale 2. Comunicazione alla famiglia 3. Nota disciplinare sul registro di classe 4. Risarcimento (anche simbolico) del danno 5. Provvedimento di carattere educativo-riparatorio 6. Riparazione diretta del danno 7. Sospensione dalle uscite didattiche con obbligo di frequenza 8.Sospensione dalle attività scolastiche con obbligo di frequenza per compiti utili a se stesso e alla comunità scolastica