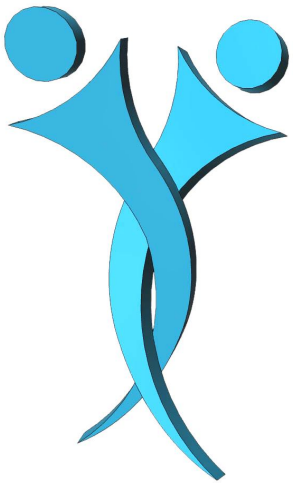


Documento di ePolicy

REIC85400A

LAZZARO SPALLANZANI

VIALE DELLA ROCCA 8 - 42019 - SCANDIANO - REGGIO EMILIA (RE)

GIACOMO LIRICI

Indice

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.

L’e-Policy è un documento programmatico steso per la prima volta nella nostra scuola che ci consentirà di promuovere le competenze ed un uso delle tecnologie digitali positivo, critico e consapevole, sia da parte degli studenti che di tutti i soggetti coinvolti nel processo educativo.

Questo percorso, quindi, fornirà indicazioni e strumenti utili all’individuazione e alla soddisfazione dei bisogni che vengono progressivamente individuati dall’Istituto e revisionati in itinere, in riferimento al tema delle tecnologie digitali in ambito educativo e didattico.

Nello specifico, è un documento programmatico elaborato appositamente dalla scuola volto a descrivere:

o il proprio approccio alle tematiche legate alle competenze digitali, alla sicurezza online e ad un uso positivo delle tecnologie digitali nella didattica;

o le norme comportamentali e le procedure per l’utilizzo delle Tecnologie dell'informazione e della comunicazione (ICT) in ambiente scolastico;

o le misure per la prevenzione;

o le misure per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

1.2 - Ruoli e responsabilità

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

Nel documento vengono definiti con chiarezza ruoli, compiti e responsabilità di ciascuna delle figure all’interno del nostro Istituto.

Il Dirigente Scolastico: Giacomo Lirici

Il Dirigente Scolastico garantisce la sicurezza, anche online, di tutti i membri della comunità scolastica, promuove la cultura della sicurezza online e contribuisce attivamente all’organizzazione di corsi di formazione specifici per tutte le figure scolastiche sull’ utilizzo positivo e responsabile delle TIC.

L’animatrice digitale: Simona Denti

L’Animatore digitale coordina la diffusione dell’innovazione attraverso l’attivazione delle attività contenute nel PNSD e previste nel PTOF del nostro Istituto.

Il Referente bullismo e cyberbullismo: Lara Dallari

Questa figura ha il compito di coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo.

Team Docente

I Docenti hanno un ruolo centrale nel diffondere la cultura dell’uso responsabile delle TIC e della Rete integrando parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l’uso delle tecnologie digitali nella didattica. Inoltre hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

Il personale Amministrativo, Tecnico e Ausiliario

Il personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste in collaborazione con il dirigente scolastico e con il personale docente e si occupa, ciascuno per la propria mansione, del funzionamento dell’Istituto scolastico che passa anche attraverso lo sviluppo della cultura digitale e dell’organizzazione del tempo scuola.

Gli Studenti e le Studentesse

Devono utilizzare in modo consapevole le tecnologie digitali, imparare a tutelarsi online, partecipare attivamente a progetti ed attività che riguardano l’uso positivo delle TIC e della rete al fine di creare competenze in materia digitale.

I Genitori

I Genitori dovrebbero relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet. È estremamente importante che accettino e condividano quanto scritto nell’e-Policy

dell'Istituto.

Gli Enti educativi esterni e le associazioni

Gli Enti educativi esterni dovrebbero conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC e promuovere comportamenti adeguati per la sicurezza online, assicurando la protezione degli studenti e delle studentesse.

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).

Il nostro istituto si impegnerà a rendere l'e-Policy uno strumento efficace per la tutela degli studenti e delle studentesse; individuando un insieme di regole da condividere con le organizzazioni o associazioni extrascolastiche e gli esperti esterni alla realizzazione di progetti ed attività educative.

La dirigenza e le figure referenti nei vari ambiti in maniera condivisa con i docenti, dovrebbero redigere un'informativa sintetica sull'e-Policy comprensiva delle procedure di segnalazione da condividere con tutte le figure che operano con studenti e studentesse. Tale documento dovrà chiarire il sistema di azioni e le procedure di segnalazione da

seguire valide anche per i professionisti e le organizzazioni esterne, finalizzate a rilevare e gestire le problematiche connesse ad un uso non consapevole delle tecnologie digitali.

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

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

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

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

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

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

Il documento di e Policy deve essere condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È importante tener presente:

o condividere e comunicare il documento agli studenti e alle studentesse significa dare loro una base di partenza per un uso consapevole e maturo dei dispositivi e della tecnologia informatica, dare loro regole condivise di sicurezza online, fornire loro elementi per poter riconoscere e quindi prevenire comportamenti a rischio, sia personali che dei/delle propri/e compagni/e.

o è importante condividere e comunicare il documento al personale scolastico in modo da poter orientare tutte le figure sui temi in oggetto, a partire da un uso corretto dei dispostivi e della Rete in linea anche con il codice di comportamento dei pubblici dipendenti;

o è fondamentale condividere e comunicare il documento ai genitori sul sito istituzionale della scuola, nonché tramite momenti di formazione specifici e durante gli

incontri scuola-famiglia.

Nella comunicazione e condivisione dell'e Policy è importante valutare i vari target di riferimento individuando i linguaggi, le modalità e i canali di comunicazione e condivisione più adatti.

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.

È necessario individuare con chiarezza le modalità di gestione di eventuali infrazioni all'e Policy.

Le possibili condotte sanzionabili sono:

o la condivisione online di immagini o video di compagni/e insegnanti senza il loro consenso o che li ritraggono in pose offensive e denigratorie;

o la condivisione di scatti intimi e a sfondo sessuale, la condivisione di dati personali, l'invio di immagini o video volti all'emarginazione di compagni/e o allo scherno di docenti e personale ATA.

A seconda dell'età è molto importante intervenire su tutto il contesto classe con attività specifiche educative e di sensibilizzazione circa l'utilizzo delle TIC e di Internet.

È opportuno valutare la natura e la gravità di quanto accaduto, al fine di considerare la necessità di denunciare l'episodio (con il coinvolgimento del Dirigente Scolastico e, se necessario, della Polizia Postale) o di garantire immediato supporto psicologico qualora ciò fosse necessario.

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.

L'e Policy dovrebbe essere riesaminata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Il monitoraggio del documento dovrebbe prevedere anche una valutazione della sua efficacia a partire dagli obiettivi specifici che lo stesso si pone da parte di un docente scelto dal Dirigente Scolastico.

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 Regolamento dell'Istituto Scolastico dovrebbe essere aggiornato con specifici riferimenti all'e Policy, inseriti nel Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

A tale proposito, sarebbe utile allegare alla ePolicy i vari regolamenti scolastici aggiornati alla luce del documento redatto.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.
- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.

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

Azioni da svolgere nei prossimi 3 anni:

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

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

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

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

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

Curricolo verticale delle competenze Digitali

La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite internet" (Raccomandazione del Parlamento Europeo in relazione alle competenze chiave per l'apprendimento permanente). Finalità delle TIC (Tecnologie dell'informazione e della Comunicazione): educare ai media. Le finalità formative delle TIC nella scuola dei tre ordini possono essere sintetizzate nei seguenti punti:

- Favorire la conoscenza dello strumento pc e/o tablet a scopo didattico.

- Sostenere l'alfabetizzazione informatica.

- Favorire la trasversalità delle discipline.

- Facilitare il processo di apprendimento.

- Favorire il processo di inclusione.

- Fornire nuovi strumenti a supporto dell'attività didattica.

- Promuovere situazioni collaborative di lavoro e di studio.

- Sviluppare creatività e capacità di lavorare in gruppo.

- Promuovere azioni di cittadinanza attiva.

- Utilizzare in modo critico, consapevole e collaborativo la tecnologia.

Competenze digitali declinate secondo le cinque aree del quadro di riferimento DIGCOMP (Quadro comune di riferimento europeo per le competenze digitali).

1. INFORMAZIONE: identificare, localizzare, recuperare, conservare, organizzare e analizzare le informazioni digitali, giudicare la loro importanza e lo scopo.

2. COMUNICAZIONE: comunicare in ambienti digitali, condividere risorse attraverso strumenti on-line, collegarsi con gli altri e collaborare attraverso strumenti digitali, interagire e partecipare alle comunità e alle reti.

3. CREAZIONE DI CONTENUTI: creare e modificare nuovi contenuti (da elaborazione testi a immagini e video); integrare e rielaborare le conoscenze e i contenuti; produrre espressioni creative, contenuti media e programmare; conoscere e applicare i diritti di proprietà intellettuale e le licenze.

4. SICUREZZA: protezione personale, protezione dei dati, protezione dell'identità digitale, misure di sicurezza, uso sicuro e sostenibile.

5. PROBLEM-SOLVING: identificare i bisogni e le risorse digitali, prendere decisioni informate sui più appropriati strumenti digitali secondo lo scopo o necessità, risolvere problemi concettuali attraverso i mezzi digitali, utilizzare creativamente le tecnologie, risolvere problemi tecnici, aggiornare la propria competenza e quella altrui.

Obiettivi

1. migliorare l'apprendimento

2. favorire l'acquisizione della competenza digitale

3. servirsi di strumenti in maniera interattiva

4. interagire in gruppi eterogenei;

5. imparare ad imparare

Competenza digitale

Scuola dell'Infanzia

Competenza	Abilità	Conoscenza
Utilizzare le nuove tecnologie per giocare, svolgere compiti, acquisire informazioni, con la guida dell'insegnante.	**•Muovere correttamente il mouse e i suoi tasti . •Utilizzare i tasti delle frecce direzionali, dello spazio, dell'invio Individuare e aprire icone relative a comandi, file, cartelle ... •Eseguire giochi ed esercizi di tipo logico, linguistico, matematico, topologico, al computer. •Prendere visione di lettere e forme di scrittura attraverso il computer Prendere visione di numeri e realizzare numerazioni utilizzando il computer. •Utilizzare la tastiera alfabetica e numerica una volta memorizzati i simboli**	**Il computer e i suoi usi Il Mouse La Tastiera**

Scuola Primaria

Competenza	Abilità	Conoscenza

- Utilizzare le TIC per lavorare con testi, immagini e suoni per rappresentare e comunicare idee **- Utilizzare diverse forme espressive dal testo alla tabella, dall'immagine al suono.** **- Utilizzare le TIC come strumento per produrre, rivedere e salvare il proprio lavoro** **- Compiere delle scelte su quali strumenti - utilizzare per produrre differenti risultati** **- Utilizzare le TIC per organizzare, classificare, gestire e presentare i lavori realizzati** **- Progettare e compiere nuovi lavori descrivendo le operazioni compiute e gli effetti ottenuti** **- Esplorare le informazioni da varie fonti riconoscendo che esse esistono in forme differenti** **- Reperire informazioni da fonti diverse** **- Utilizzare le TIC per comunicare** **- Riflettere e valutare le esperienze con le TIC sia all'interno della scuola che all'esterno.**	**• Riconoscere e documentare le funzioni principali di una nuova applicazione informatica.** **• Rappresentare i dati dell'osservazione attraverso tabelle, mappe, diagrammi, disegni.** **• Organizzare una gita o una visita ad un museo usando internet per reperire notizie e informazioni.** **• Utilizzare semplici procedure per la selezione, la preparazione e la presentazione degli alimenti.** **• Eseguire interventi di decorazione, riparazione e manutenzione sul proprio corredo scolastico.** **• Realizzare un oggetto in cartoncino descrivendo e documentando la sequenza delle operazioni.** **• Cercare, selezionare, scaricare e installare sul computer un comune programma di utilità** **• Utilizzare software offline e online per attività di Coding**	**- Le principali parti e funzioni del computer** **- Le funzioni di base di un personal computer e di un sistema operativo: le icone, le finestre di dialogo, le cartelle, i file.** **- Semplici programmi di grafica e/o giochi didattici.** **- Le funzioni di base dei programmi di videoscrittura per la produzione di semplici testi** **- Le funzioni base dei programmi di presentazione per la rappresentazione dei lavori realizzati** **- Le funzioni di base di un foglio elettronico per la creazione di tabelle e grafici** **- La stampa dei documenti - Navigazione in una rete locale, accesso alle risorse condivise, scambio di documenti** **- Il collegamento ad Internet attraverso un browser e navigazione di alcuni siti selezionati** **La navigazione in Internet: le regole e le responsabilità** **- Motori di ricerca** **- Costruzione di semplici documenti ottenuti collegando tra loro informazioni provenienti da sorgenti diverse** **- La posta elettronica per lo scambio di semplici messaggi** **- Concetti base del Coding** **- Il blog come strumento per comunicare** **- Classroom come classe virtuale**

Scuola Secondaria di primo grado

Competenza	Abilità	Conoscenza

-Utilizzare con dimestichezza le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall'attività di studio. **-Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, con particolare riferimento al contesto produttivo, culturale e sociale in cui vengono applicate.** **-Saper gestire la propria e-safety** **-Saper utilizzare la tecnologia per sviluppare il pensiero computazionale e per realizzare simulazioni, modellizzazioni, quiz, esercizi, ec...**	**• Utilizzare le Tecnologie dell'Informazione e della Comunicazione per elaborare dati, testi, immagini, video, per produrre artefatti digitali (comprese le modellizzazioni) in diversi contesti e per la comunicazione.** **• Conoscere gli elementi base che compongono un computer e le relazioni essenziali fra di essi.** **• Collegare le modalità di funzionamento dei dispositivi elettronici con le conoscenze scientifiche e tecniche acquisite.** **• Utilizzare materiali digitali per l'apprendimento** **• Utilizzare il PC, periferiche e programmi applicativi** **• Riconoscere potenzialità e rischi connessi all'uso delle tecnologie e della Rete, saper gestire i propri account in funzione della e-safety** **• Utilizzare software offline e online per attività di Coding.**	**- Le applicazioni tecnologiche quotidiane e le relative modalità di funzionamento, in particolare Google Documenti, Google Fogli e Google Presentazioni.** **- I dispositivi informatici di input e output** **- Il sistema operativo, i software e le apps, applicativi (residenti e/o cloud), con particolare riferimento ai prodotti anche Open source.** **- Procedure per la produzione/elaborazione di testi, dati e immagini, prodotti multimediali** **- Procedure di utilizzo delle Reti per la ricerca di informazioni, per la comunicazione, la collaborazione e la condivisione.** **- Procedure di utilizzo sicuro e legale della Rete per la ricerca e la condivisione di dati (motori di ricerca, sistemi di comunicazione mobile, email, chat, social network, cloud, protezione degli account, download, diritto d'autore, ecc.)** **Fonti di pericolo e procedure di sicurezza. E-safety** **- Concetti base del coding**

Metodologie

1. **lezioni on line,**
2. **cooperative learning**
3. **problem solving**
4. **lezioni interattive con l'utilizzo della LIM o altri devices (pc, tablet, smartphone...)**
5. **sviluppo di mappe mentali per l'organizzazione delle conoscenze attraverso i tools Bubbleus /Cmap etc...**

6. web quest

7. sviluppo del pensiero computazionale

8. lavoro di gruppo con produzione digitale

Ruoli

L'insegnante	Lo studente	La scuola
1. Progetta percorsi che prevedono la condivisione di risorse in A.V. (aula virtuale) **2. Posta le lezioni in A.V.** **3. Utilizza abitualmente le mappe mentali e cognitive in classe** **4. Predispone materiale ed esercitazioni in A.V.** **5. Corregge i compiti in A.V.** **6. Utilizza e richiede l'utilizzo delle TIC** **7. Prevede l'utilizzo dei vari digital device ma accetta il lavoro anche in formato cartaceo.** **8. Frequenta i corsi di aggiornamento proposti**	**1. Segue i percorsi virtuali** **2. Utilizza i tools proposti dall'insegnante** **3. Utilizza la tecnologia richiesta** **4. Esegue i compiti in formato digitale quando richiesto** **5. Collabora con i pari**	**1. Mette a disposizione attrezzature tecnologiche aggiornate** **2. Attrezza i vari plessi di connessione a banda larga** **3. Mette a disposizione docenti preparati sulle TIC** **4. Ha un responsabile esperto che si preoccupa di risolvere eventuali problematiche** **5. Predispone percorsi di formazione professionale**

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.

Le TIC devono essere usate dagli insegnanti ad integrazione della didattica al fine di

progettare, sviluppare, utilizzare, gestire e valutare i processi di insegnamento e apprendimento di tutti gli studenti e le studentesse della classe compresi gli alunni disabili. Il loro utilizzo infatti non solo può rendere gli apprendimenti motivanti, coinvolgenti ed inclusivi, ma permette al docente di guidare studenti e studentesse rispetto alla fruizione dei contenuti online e permettono di sviluppare capacità che sono sempre più importanti anche in ambito lavorativo. Di conseguenza, gli insegnanti stessi devono impegnarsi a raggiungere un buon livello di formazione in merito all'utilizzo e all'integrazione delle TIC nella didattica, attraverso la partecipazione del personale ad iniziative coerenti con il piano di formazione.

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.

Al fine 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 maggior parte dei docenti dell'Istituto scolastico sarà indirizzato verso un percorso formativo specifico ed adeguato che abbia ad oggetto non solo l'uso responsabile e sicuro della Rete ma anche i rischi legati ad essa.

Per tali ragioni, l'Istituto prevede specifici momenti di formazione per gli insegnanti a partire dall'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica, prevedendo l'inserimento di tali azioni programmatiche nel Piano triennale dell'offerta formativa (PTOF) in un'ottica di programmazione specifica:

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

o Promuovere la partecipazione dei docenti a corsi di formazione che abbiano ad oggetto i temi del progetto "Generazioni Connesse";

o Monitorare le azioni svolte per mezzo di specifici momenti di valutazione;

o Organizzare incontri con professionisti della scuola o con esperti esterni, enti/associazioni.

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

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

Il "Patto di Corresponsabilità" è un documento centrale per ogni istituzione scolastica e per la comunità educante, per sensibilizzare le famiglie si aggiornerà e si integrerà perciò con specifici riferimenti alle tecnologie digitali e all'e-Policy. In questo modo si informano i genitori sulle condotte che si adottano a scuola e offrire consigli di buone pratiche, ma anche metterli a conoscenza dei rischi connessi ad un uso distorto della rete.

Nel documento si sottolinea:

o l'elaborazione delle regole sull'uso delle tecnologie digitali da parte dei genitori nelle comunicazioni con la scuola e con i docenti (es. mail, gruppo whatsapp, sito della scuola etc.) e informarli adeguatamente anche riguardo alle regole per gli studenti e le studentesse;

o l'organizzazione di percorsi di sensibilizzazione e formazione dei genitori su un uso responsabile e costruttivo della Rete in famiglia e a scuola.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni

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

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

Scegliere almeno 1 di queste azioni

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

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

personali.

LIBERATORIA PRIVACY

Per le informative legate alla Privacy e le liberatorie per l'utilizzo delle immagini si rimanda alla sezione Privacy del sito di istituto, raggiungibile da questo link: http://www.icspallanzani.edu.it/2013-12-26-12-31-46.html

---

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.

Viste le norme di riferimento in parte sopracitate nel testo standard e considerato il patto formativo del nostro istituto, il regolamento della scuola e il PTOF

Si stilano i seguenti punti per regolare l'accesso a internet di tutti i soggetti coinvolti e per garantire questo diritto fondamentale:

Nomina dell'Amministratore di sistema e del Custode delle password: Franco Iannece e Simona Denti

Il datore di lavoro conferisce all'Amministratore di sistema il compito di sovrintendere alle risorse informatiche dell'Istituto assegnandogli le seguenti attività:

a) gestione dell'hardware e del software (installazione, aggiornamento, rimozione) di tutte le strutture tecniche informatiche dell'istituto, siano esse collegate in rete o meno;

b) configurazione dei servizi di accesso alla rete interna, ad internet e a quelli di posta elettronica con creazione, attivazione e disattivazione dei relativi account;

c) attivazione della password di accensione (BIOS);

d) creazione di un'area condivisa sul server per lo scambio di dati tra i vari utenti, evitando condivisioni dei dischi o di altri supporti configurati nel PC che non siano strettamente necessarie perché sono un ottimo "aiuto" per i software che cercano di "minare" la sicurezza dell'intero sistema;

e) controllo del corretto utilizzo delle risorse di rete, dei computer e degli applicativi, durante le normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

f) rimozione sia sui PC degli incaricati sia sulle unità di rete, di ogni tipo di file o applicazione che può essere pericoloso per la sicurezza o costituisce violazione del presente regolamento;

g) distruzione delle unità di memoria interne alla macchina (hard - disk, memorie allo stato solido) ogni qualvolta si procederà alla dismissione di un PC e dei supporti removibili consegnati a tale scopo dagli utenti;

h) utilizzo delle credenziali di amministrazione del sistema per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di indispensabile ed indifferibile necessità di intervento per prolungata assenza, irrintracciabilità o impedimento dello stesso, solo per il tempo necessario al compimento di attività indifferibili e solo su richiesta del Responsabile del trattamento.

L'Amministratore di sistema, nell'espletamento delle sue funzioni legate alla sicurezza e

alla manutenzione informatica, ha facoltà di accedere in qualunque momento, anche da remoto, e dopo aver richiesto l'autorizzazione all'utente interessato, al PC di ciascun utente. Il Custode delle password è incaricato di custodire e conservare in luogo riservato e sicuro, in formato cartaceo, le credenziali. E' tenuto a ottemperare al suo compito avendo cura di non diffondere, nemmeno accidentalmente, le stesse a persone estranee al loro utilizzo.

Assegnazione delle postazioni di lavoro

Per ridurre il rischio di impieghi abusivi o dannosi, il datore di lavoro o chi preposto per esso provvede a:

-individuare preventivamente le postazioni di lavoro e assegnarle a ciascun dipendente,

-individuare preventivamente gli utenti a cui è accordato l'utilizzo della posta elettronica e l'accesso a internet. La strumentazione dell'Istituto non è di esclusivo dominio del dipendente, ma rientra tra i beni a cui determinati soggetti possono comunque sempre accedere. L'eventuale accesso del datore di lavoro, qualora necessiti di informazioni contenute nei documenti residenti sul PC assegnato al dipendente, è legittimo.

Utilizzo dei personal computer e della LIM

Gli utenti utilizzano per il proprio lavoro soltanto computer di proprietà dell'Istituto di cui sono responsabili, salvo eccezioni autorizzate dal datore di lavoro. Sono tenuti a:

• applicare al PC portatile le regole di utilizzo previste per i PC connessi in rete,

• custodirlo con diligenza e in luogo protetto durante gli spostamenti,

• rimuovere gli eventuali file elaborati sullo stesso prima della sua riconsegna,

• non disattivare sul PC lo screen saver e la relativa password,

• conservare la password nella massima riservatezza e con la massima diligenza,

• non modificare la configurazione hardware e software del PC se non esplicitamente autorizzati dall'amministratore di sistema,

• non rimuovere, danneggiare o asportare componenti hardware,

• nel caso il software antivirus rilevi la presenza di un virus, sospendere immediatamente ogni elaborazione in corso, senza spegnere il PC e segnalare prontamente l'accaduto al personale incaricato dell'assistenza tecnica,

• permettere l'autoaggiornamento del PC,

• utilizzare con cura la LIM;

• non accedere ai PC delle LIM durante le pause ricreative e senza che vi sia la supervisione di un docente;

• comunicare tempestivamente al referente informatico dell'istituto qualsiasi rottura o inefficienza;

• prestare la massima attenzione ai supporti di origine esterna (es. pendrive), verificando preventivamente, tramite il programma antivirus, ogni file acquisito attraverso qualsiasi supporto e avvertendo immediatamente il responsabile informatico della sede e/o l'Amministratore di sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti, ed utilizzarla il minimo possibile;

non lasciare incustodita e accessibile la propria postazione una volta eseguita la connessione al sistema con le proprie credenziali di autenticazione,

• non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a persone non autorizzate, in particolar modo per quanto riguarda l'accesso ad internet e ai servizi di posta elettronica,

• spegnere il PC al termine del lavoro o in caso di assenze prolungate dalla propria postazione.

Utilizzo di supporti magnetici

Tutto il personale è invitato a non utilizzare dispositivi di memoria esterna (chiavi USB, CD, DVD, ecc.) ma ad utilizzare i Repository su Cloud del dominio @icspallanzani.org

Qualora sia indispensabile l'utilizzo di supporti magnetici, gli utenti devono averne particolare cura (Disposizioni anticipate di trattamento, chiavi USB, CD riscrivibili,...) in particolar modo quelli riutilizzabili, per evitare che persone non autorizzate possano accedere ai dati qui contenuti. Di conseguenza le azioni da compiere obbligatoriamente sono le seguenti:

a) porre attenzione nell'utilizzo dei supporti rimovibili personali,

b) custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto,

c) consegnare i supporti magnetici riutilizzabili (DAT, chiavi USB, CD riscrivibili, ...) obsoleti all'Amministratore di sistema per l'opportuna distruzione onde evitare che il loro contenuto possa essere successivamente recuperato in seguito alla cancellazione.

Utilizzo delle stampanti e dei materiali d'uso

Stampanti e materiali di consumo in genere (carta, inchiostro, toner, supporti digitali come CD e DVD) possono essere usati esclusivamente per compiti di natura strettamente istituzionale, evitando in ogni modo sprechi e utilizzi eccessivi. Gli utenti devono effettuare la stampa dei dati solo se strettamente necessaria e ritirare prontamente dai vassoi delle stampanti comuni i fogli per impedire a persone non autorizzate di accedere alle stampe di documenti riservati, distruggere personalmente e sistematicamente le stampe che non servono più.

Utilizzo di telefonini e altre apparecchiature

Il telefono del dipendente, nell'orario di permanenza a scuola, non è considerato uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo

svolgimento delle attività lavorative ma non durante l'orario di docenza, e non sono quindi consentite comunicazioni a carattere personale. La ricezione o l'effettuazione di telefonate personali sono consentite solo nel caso di comprovata necessità ed urgenza, mediante il telefono fisso a disposizione della scuola. È vietato l'utilizzo del fax e delle fotocopiatrici d'Istituto per fini personali.

ISTITUTO COMPRENSIVO "LAZZARO SPALLANZANI"

Viale della Rocca 8 - Scandiano (RE)

0522-857593 www.icspallanzani.edu.it reic85400a@istruzione.it reic85400a@pec.istruzione.it

Regolamento BYOD - Bring Your Own Devices - Porta il tuo dispositivo a scuola

Regolamento per l'utilizzo dei dispositivi digitali personali a scuola

L'azione #6 del PNSD "Politiche attive per il BYOD" (Bring your own device), - letteralmente: porta il tuo dispositivo - punta a garantire a tutti gli studenti una formazione digitale che parta dal saper usare i propri dispositivi. Si legge testualmente "La scuola digitale, in collaborazione con le famiglie e gli enti locali, deve aprirsi al cosiddetto BYOD (Bring Your Own Device), ossia a politiche per cui l'utilizzo di dispositivi elettronici personali durante le attività didattiche sia possibile ed efficientemente integrato". Poiché la tecnologia fornisce agli studenti opportunità innovative ed inedite per incrementare la loro cultura, in linea con quanto specificato nel PNSD, il nostro Istituto intende favorire tale processo garantendone la sicurezza attraverso una modalità di interazione che

contribuisca al miglioramento dell'ambiente educativo e di apprendimento. Pertanto l'uso improprio dei dispositivi digitali mobili a scuola è inaccettabile e viene sanzionato in misura della gravità in base a quanto stabilito dal Regolamento di Istituto.

1. Dispositivi ammessi: notebook con installato il browser Chrome, chromebook, tablet con installato il browser Chrome, fotocamera digitale, lettori e registratori audio e/o video.

2. I dispositivi devono essere usati a scuola per soli scopi didattici e solo dopo previa autorizzazione esplicita dell'insegnante (regola del semaforo). Agli studenti non è permesso usarli per giochi o attività diverse da quelle didattiche durante le ore scolastiche o durante le le pause ricreative.

3. E' vietato agli studenti usare dispositivi di registrazione audio, videocamere o fotocamere (o dispositivi che li prevedano) per registrare media o fare foto in classe senza il permesso dell'insegnante e senza il consenso della persona che viene registrata.

4. Audio e video registrati a scuola a fini didattici possono essere pubblicati esclusivamente in canali di comunicazione intestati ufficialmente all'I.C. Spallanzani.

5. Gli studenti sono responsabili personalmente dei propri dispositivi; è vietato prendere in prestito dispositivi di altri studenti.

6. La scuola non è responsabile della sicurezza dei dispositivi e di eventuali danni.

7. Gli studenti sono responsabili di riportare a casa il dispositivo al termine delle lezioni. La scuola non sarà ritenuta responsabile per nessun dispositivo degli studenti lasciato a scuola.

8. Uso non consentito di Internet:

a. Usare Internet per scopi diversi da quelli didattici;

b. Scaricare musica, video e programmi da internet o qualsiasi file senza il consenso

dell'insegnante;

c. Giocare sul computer, in rete o diversamente (se non come parte di una lezione);

d. usare dispositivi audio, video o fotografici per ritrarre qualsiasi persona durante l'attività didattica per scopi diversi da quelli didattici, se non ha ottenuto il permesso esplicito del docente e se non ha autorizzato tale attività.

9. Agli studenti è richiesto di caricare completamente le batterie del proprio dispositivo a casa e devono essere consapevoli che:

a. non sarà possibile ricaricare i dispositivi durante l'orario di lezione;

b. non sarà possibile ricaricare i dispositivi in aula; a tal scopo si consiglia di dotarsi di

caricabatteria portatili e di portare il dispositivo completamente carico a scuola.

10. Diritti di proprietà intellettuale:

Gli studenti devono rispettare e proteggere la proprietà intellettuale altrui:

• Non è ammessa la copia o il plagio di qualsiasi materiale;

• Non è ammessa la violazione dei copyrights;

• Si deve attribuire, citare e richiedere il permesso degli autori o creatori delle informazioni o dei media originali (se richiesto dalla legge o da accordo).

11. Diritto di ispezione

• La scuola si riserva il diritto di monitorare le attività online degli utenti.

• La scuola può ispezionare la memoria del dispositivo dello studente se ritiene che le regole scolastiche non siano state rispettate, questo comprende, ma non è limitato, a registrazioni audio e video, fotografie scattate nelle pertinenze scolastiche e che violano la privacy altrui, o ogni altra questione legata a cyberbullismo, ecc.

12. Sanzioni per il mancato rispetto del Regolamento: L'accesso al network della scuola è un privilegio, non un diritto. L'uso della tecnologia, sia essa proprietà della scuola o un dispositivo fornito dagli studenti, comporta responsabilità personali. Ci si aspetta che gli studenti rispettino le regole dell'I.C., agiscano responsabilmente e onorino i termini e le condizioni fissate dall'insegnante di classe e dalla scuola. Il mancato rispetto di questi termini e condizioni potrà risultare nella temporanea perdita di accesso alla rete nonché altre azioni disciplinari e legali, se necessario. Gli studenti saranno ritenuti responsabili delle loro azioni e sono incoraggiati a segnalare immediatamente ogni uso accidentale al loro insegnante. Le sanzioni dipenderanno dalla gravità dell'accaduto e sanzionate secondo il Regolamento di Istituto. I dispositivi potranno essere confiscati per l'intera giornata.

Oggetto: PATTO BYOD

(Bring Your Own Device - Porta il tuo dispositivo)

Carissimo/a alunno/a, come studente/essa della classe ……. sez. ….…. del plesso…… avrai la possibilità di poter portare da casa a scuola il tuo device. Questa opportunità comprende anche alcune regole.

Leggi bene il seguente patto perché, se non rispetterai queste regole, ti verrà tolta tale possibilità.

1. Non sei obbligato a portare a scuola il tuo device.

2. I tuoi genitori devono essere informati dell'utilizzo del dispositivo a scuola.

3. Il device personale verrà utilizzato a scuola solo quando richiesto dagli insegnanti.

4. La tipologia di device sarà preventivamente concordata con l'insegnante.

5. Utilizzerai il device esclusivamente per scopi didattici, seguendo il regolamento della scuola e le indicazioni degli insegnanti.

6. Ricorda che il BYOD è un privilegio che può essere revocato.

7. Se userai impropriamente il device, ti verrà ritirato.

8. Non puoi utilizzare i dispositivi nei bagni, negli spogliatoi, nei corridoi, durante gli spostamenti e l'intervallo e, comunque, in ogni situazione se non autorizzato dagli insegnanti.

9. Collega sempre il tuo dispositivo alla rete wi-fi della scuola per navigare in un ambiente protetto.

10. Se porti il tuo dispositivo, devi assicurarti che sia carico.

11. Il tuo dispositivo è sotto la tua responsabilità, usalo solo per scopi didattici, conservalo in sicurezza, utilizzalo rispettando le regole dei tuoi genitori e della scuola.

12. Utilizza il tuo dispositivo in modo significativo e opportuno dal punto di vista didattico e rispettoso delle leggi europee e dello Stato.

13. Rispetta le regolamentazioni sulla Privacy e i diritti delle persone che ti circondano.

14. Rispetta la regola del semaforo.

ROSSO All'inizio della lezione i dispositivi devono essere spenti; no silenzioso; no vibrazione.
GIALLO I dispositivi devono essere messi a faccia in giù (stand by) a lato del banco. Devono essere in modalità silenziosa o vibrazione. I dispositivi possono essere toccati solo con il consenso dell'insegnante.
VERDE Gli studenti possono tenere sul banco i dispositivi e usarli quando vogliono nel rispetto delle regole e della finalità didattica. Gli studenti devono tenere i dispositivi in modalità silenziosa.

Per consenso e accettazione.

Luogo e data:_____ Firma dell'alunno/a Firma dei genitori/tutori

DICHIARAZIONI DEI GENITORI/TUTORI LEGALI

I sottoscritti _____ e _____ tutori legali dell'alunno/a _____ frequentante la classe _____ sez. ____ della scuola _____

DICHIARANO:

1. di essere al corrente che, in ambito scolastico, i docenti potranno introdurre, a fianco degli strumenti e dei materiali didattici in uso a scuola, l'utilizzo di applicazioni, contenuti e servizi fruibili in locale e in Internet tramite dispositivi elettronici propri;

2. di collaborare con i docente nel responsabilizzare i ragazzi sulle modalità di accesso a Internet e sulle regole a cui attenersi;

3. che durante la permanenza a scuola del dispositivo il/la proprio/a figlio/a sarà il/la solo/a responsabile della sua custodia e del suo uso corretto, secondo le regole e le disposizioni concordate con gli insegnanti.

AUTORIZZANO IL/LA PROPRIO/A FIGLIO/A a portare a scuola il proprio device* secondo la

modalità e la tipologia concordata con l'insegnante.

Luogo e data _____ Firma dei genitori/tutori legali _____

***I device consentiti a scuola sono notebook con installato il browser Chrome, chromebook, tablet con installato il browser Chrome, fotocamera digitale, lettori e registratori audio e/o video.**

Utilizzo della rete informatica

Le reti interne, presenti in ciascuno dei vari plessi scolastici, collegano tutti i computer presenti in ogni singolo edificio.

Utilizzo delle password

Per l'accesso alla strumentazione informatica di Istituto ciascun utente deve essere in possesso delle specifiche credenziali di autenticazione previste ed attribuite dall'incaricato della custodia delle password. Le credenziali di autenticazione per l'accesso alla rete consistono in un codice per l'identificazione dell'utente (user id) associato ad una parola chiave (password) riservata che dovrà essere custodita dal Custode delle password con la massima diligenza e non può essere divulgata. Anche l'utente si deve impegnare nella cura della custodia della password.

Utilizzo di internet

La navigazione in internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa e alla crescita dello studente. L'accesso ad internet è regolato da filtri predefiniti dall'amministratore di sistema su autorizzazione dell'amministrazione, con esclusione dei siti istituzionali. L'Amministratore di sistema provvede alla configurazione di sistemi e all'utilizzo di filtri che prevengono determinate operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di file o software).

L'accesso alla navigazione in internet deve essere effettuato esclusivamente a mezzo della rete di istituto e solo per fini lavorativi o di studio. Gli utenti sono tenuti ad utilizzare l'accesso ad internet in modo conforme a quanto stabilito dal presente regolamento e quindi devono navigare solamente in siti attinenti allo svolgimento delle mansioni assegnate.

Agli utenti è fatto espresso divieto di qualsiasi uso di internet che possa in qualche modo recare danno all'istituto o a terzi e quindi di:

a) fare conoscere ad altri la password del proprio accesso,

b) usare internet per motivi personali,

c) servirsi dell'accesso internet per attività in violazione del diritto d'autore o di altri diritti

tutelati dalla normativa vigente,

d) accedere a siti pornografici e di intrattenimento

e) scaricare i software gratuiti dalla rete, salvo casi di comprovata utilità e previa autorizzazione in tal senso da parte del dirigente,

f) utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer (Napster, Emule, Winmx, e-Donkey,...)

g) ascoltare la radio o guardare video o filmati utilizzando le risorse internet, se non attinenti l'attività lavorativa o di studio;

h) effettuare transazioni finanziarie, operazioni di remote banking, acquisti on-line e simili, se non attinenti l'attività lavorativa o direttamente autorizzati dal Responsabile del trattamento,

i) inviare fotografie, dati personali o di amici dalle postazioni internet. Al termine dell'utilizzo della rete è obbligatorio effettuare il logout.

Utilizzo della posta elettronica

L'istituto mette a disposizione dei lavoratori e degli studenti indirizzi di posta elettronica individuali in dominio istituzionale @icspallanzani.org (servizio di posta interno all'Istituto) che consentono:

- di inviare e ricevere comunicazioni attinenti allo svolgimento dell'attività lavorativa, - di partecipare a gruppi di lavoro in condivisione e collaborazione, attinenti allo svolgimento dell'attività lavorativa o di studio.

Tramite

la posta istituzionale con dominio @icspallanzani.org possono essere trasmesse le seguenti comunicazioni:

- convocazioni riunioni;

- comunicazioni di servizio anche dirette al singolo dipendente;

- materiale relativo alle decisioni prese nelle riunioni collegiali;

- circolari;

-Materiali di studio;

- compiti;

-verifiche ;

- copia elettronica di documenti redatti su supporti cartacei (purché in formati e

dimensioni opportune).

Ogni utente assegnatario di una casella di posta elettronica istituzionale (alunni, docenti, personale ATA e DS) è responsabile del corretto utilizzo della stessa ed è tenuto a utilizzarla in modo conforme a quanto stabilito dal presente regolamento, quindi deve: a) conservare la password nella massima riservatezza e con la massima diligenza, b) mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti, c) utilizzare l'account per l'invio di comunicazioni attinenti all'attività lavorativa e di studio e) al termine delle operazioni effettuare il logout dall'account.

Agli utenti è fatto divieto di qualsiasi uso della posta elettronica che possa in qualche modo recare danno all'istituto o a terzi e quindi di: a) prendere visione della posta altrui, b) simulare l'identità di un altro utente, ovvero utilizzare per l'invio di messaggi credenziali di posta non proprie, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza, c) utilizzare strumenti software o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all'interno dell'istituto, d) trasmettere a mezzo posta elettronica dati sensibili, personali o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento della protezione dei dati, e) utilizzare il servizio di posta elettronica per inoltrare giochi, scherzi, barzellette, appelli e petizioni, messaggi tipo "catene" e altre e-mail che non siano di lavoro o a fini di studio.

Gestione del sito Web della scuola

L'Istituzione Scolastica possiede un Sito Web per la gestione della parte didattica del quale viene nominato referente un docente per ogni plesso. In nessun caso l'Istituto potrà essere ritenuto responsabile dei danni di qualsiasi natura causati direttamente o indirettamente dall'accesso al sito, dall'incapacità o impossibilità di accedervi, dall'affidamento dell'utente e dall'utilizzo dei contenuti. L'Istituto provvederà ad inserire nel sito informazioni e comunicazioni aggiornate, servizi, notizie, eventi, articoli relativi alle attività didattiche dell'Istituto, documenti e albo, contatti e orari.

L'Istituzione Scolastica possiede un registro elettronico gestito dall' Amministratore. Tutti i dati relativi agli utenti che utilizzano il software sono protetti da password e sarà compito di ogni utente conservare e custodire le proprie credenziali.

Diritti e responsabilità dei dipendenti

Per assicurare la tutela dei diritti, delle libertà fondamentali e della dignità dei lavoratori, garantendo che sia assicurata una protezione della loro sfera di riservatezza nelle relazioni personali professionali, il trattamento dei dati mediante l'uso delle tecnologie telematiche è conformato al rispetto dei diritti delle libertà fondamentali nonché della dignità dell'interessato, dei divieti posti dallo statuto dei lavoratori sul controllo a distanza e dei principi di necessità, correttezza e finalità determinate, esplicite e legittime. Ogni utente è responsabile, sia sotto il profilo civile che penale, del corretto uso delle risorse informatiche, dei servizi e dei programmi ai quali ha accesso e dei dati che tratta. Spetta ai docenti vigilare affinché gli studenti loro affidati rispettino il regolamento e ne siano

direttamente responsabili.

Referente informatico dell'istituto

Il DS nomina il referente il referente informatico di ogni plesso. Il personale docente e ATA è tenuto a comunicare tempestivamente qualsiasi rottura o inefficienza del sistema informatico, ed il referente, se con le proprie conoscenze personali non riesce a risolverli, deve comunicare tramite l'ufficio di segreteria addetto la necessità al tecnico informatico designato dal datore di lavoro. Deve comunicare altresì eventuali rotture irrisolvibili per pianificare nuovi acquisti a tale ufficio.

Doveri di comportamento dei dipendenti e degli alunni

Le strumentazioni informatiche , se personali, la rete internet e la posta elettronica devono essere utilizzate dagli studenti sotto il controllo dei loro docenti, come strumenti di lavoro e studio. Ogni loro utilizzo non inerente l'attività lavorativa e didattica è vietato in quanto può comportare disservizi, costi di manutenzione e soprattutto minacce alla sicurezza e della privacy dell'alunno e del personale.

In particolare non può essere dislocato nelle aree di condivisione della rete alcun file che non sia legato all'attività lavorativa o didattica, nemmeno per brevi periodi. Agli utenti è severamente vietata la memorizzazione di documenti informatici di natura oltraggiosa o discriminatoria per sesso, lingua, religione, razza, origine etnica, condizioni di salute, opinioni, appartenenza sindacale politica. Non è consentito scaricare, scambiare o utilizzare materiale coperto dal diritto d'autore o ritrarre qualsiasi persona che non abbia autorizzato riprese audio, video o fotografiche, che non coincidano con esigenze lavorative e didattiche e che non siano autorizzate dal DS e dal docente. L'utilizzo errato è sanzionato dal regolamento scolastico e dalla legge vigente.

3.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

Gli strumenti utilizzati per la comunicazione online sono: il registro elettronico, la mail, le

Google Suite for Education per l'apprendimento di @icspallanzani.org (dominio applicativo), web radio dell'Istituto e programmi autorizzati dai genitori e normati dalla legge sulla Privacy vigente.

E' importante ricordare che l'art. 22 del CCNL 2016/2018 (diritto alla disconnessione), fornisce i criteri generali per l'utilizzo di strumentazioni tecnologiche in orario diverso da quello di servizio per conciliare al meglio vita lavorativa e familiare.

Per le chat informali (fra colleghi, docenti e genitori) non esiste una vera e propria regolamentazione, pertanto sarebbe opportuno attenersi alle seguenti norme di buon senso:

- **comprendere e rispettare la finalità del gruppo, scrivendo o pubblicando solo contenuti pertinenti;**
- **usare un linguaggio adeguato, chiaro e preciso;**
- **evitare di affrontare in chat argomenti troppo complessi e controversi;**
- **evitare discussioni che riguardano solo pochi membri della chat;**
- **non condividere file multimediali pesanti;**
- **non condividere foto di studenti in chat;**
- **fare domande precise e chiare a cui è possibile rispondere in modo breve e preciso;**

Il registro elettronico permette la comunicazione con le famiglie sull'andamento scolastico, i colloqui, gli eventi, i risultati scolastici e comunicazioni varie.

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.

Ad oggi il nostro istituto non ha approvato l'uso del BYOD, ma è stato stilato un regolamento che sarà proposto durante il prossimo anno scolastico al Collegio Docenti. Si è pensato a questo regolamento, già esposto al punto 3.2.

https://docs.google.com/document/d/1uUbWYn3NMfkgHQ0SvU5X0Pu4E92gf9yqb3JUmtDBFA0/edit?usp=sharing

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

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

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

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

Scegliere almeno 1 di queste azioni:

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

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

Parlando di sensibilizzazione si tratta in questi casi di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento.

Molte campagne di sensibilizzazione hanno, ad esempio, una risonanza internazionale che può mirare a:

- **mettere in luce una determinata problematica o condizione,**

- **chiedere ad una determinata utenza di attivarsi per una causa,**
- **raccogliere dei fondi.**

Altri interventi possono, invece, essere mirati a piccoli gruppi o comunità (come ad esempio la comunità scolastica), con l'obiettivo di coinvolgere un gruppo ristretto di persone affinché agiscano insieme in favore di una causa in cui credono.

Parlando di prevenzione in ambito digitale si potrebbe tradurre quanto appena detto con un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

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

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

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
    - Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo.

A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
- Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Il nostro istituto, attraverso la stesura di questo documento programmatico, si impegna a prevenire e intervenire su atti di bullismo e cyberbullismo attraverso tutte le linee individuate in questa E Policy e mediante la diffusione dello stesso a tutti i soggetti coinvolti.

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

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

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

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

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

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti…) 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, etc.) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, negli ultimi anni si è fortemente diffuso e rafforzato soprattutto attraverso l'uso della Rete, i social network in particolar modo, dove non è difficile e infrequente trovare forme di odio e hate speech online particolarmente violente. Il nostro istituto si impegna, in particolare nella scuola secondaria di primo grado, a far conoscere questo fenomeno agli alunni, riflettendoci direttamente con gli alunni attraverso le discipline antropologiche e scientifiche, ma anche attraverso l'acquisizione di un codice etico, patrimonio acquisibile in modo interdisciplinare. Si interverrà anche con specifici progetti mirati alle dinamiche del cyberbullismo.

Scopriamo insieme le caratteristiche dell'hate speech, come riconoscerlo e prevenirlo, a partire dal documento No hate Ita (che vi invitiamo a leggere integralmente per un ulteriore approfondimento):

- **Il discorso d'odio procura sofferenza. La parola ferisce, e a maggior ragione l'odio! Il discorso può violare i diritti umani. Il discorso d'odio online non è meno grave della sua espressione offline, ma è più difficile da individuare e da combattere.**

- **Gli atteggiamenti alimentano gli atti. Il discorso dell'odio è pericoloso anche perché può condurre a più gravi violazioni dei diritti umani, e perfino alla violenza fisica. Può contribuire a inasprire le tensioni razziali e altre forme di discriminazione e di violenza.**

- **L'odio online non è solo espresso a parole. Internet ci permette di comunicare rapidamente e in modi svariati, ad esempio, mediante i social media e i giochi online, molto spesso, d'altronde, in maniera anonima. L'odio online può esprimersi sotto forma di video e foto, come pure, più solitamente, di contenuto testuale. Le forme visive o multimediali hanno sovente un impatto più forte sugli atteggiamenti (consci e inconsci).**

- **L'odio prende di mira sia gli individui che i gruppi. L'odio online può prendere di mira dei gruppi che spesso sono già vulnerabili sotto altri aspetti, come i richiedenti asilo, le minoranze religiose o le persone con disabilità. Tuttavia, anche i singoli individui sono sempre maggiormente oggetto di attacchi. Le conseguenze sono talvolta fatali, come dimostrato da numerosi fatti di cronaca riferiti dai media, riguardanti giovani vittime di cyberbullismo che sono state spinte al suicidio.**

- **Internet è difficilmente controllabile. La diffusione di messaggi di incitamento**

all'odio è maggiormente tollerata su Internet rispetto al mondo offline ed è sottoposta a minori controlli. È ugualmente più facile (e comporta meno rischi) insultare o molestare online, perché le persone spesso si esprimono sotto la copertura dell'anonimato.

- **Ha radici profonde. Gli atteggiamenti e le tensioni sociali che suscitano sentimenti di odio online affondano le loro radici nella società, e non sono diversi, in genere, da quelli che alimentano il discorso dell'odio offline.**

- **Impunità e anonimato. Sono le due presunte caratteristiche delle interazioni sociali in rete: l'impunità e l'anonimato. Queste abbassano le remore etiche. In realtà, però, qualsiasi azione compiuta sul web consente di rintracciare il suo autore.**

Il discorso dell'odio si manifesta con un ampio spettro di azioni: sebbene tutte le espressioni che istigano all'odio meritino di essere classificate come malvagie, ne esistono alcune che possono essere peggiori di altre. È utile, quindi, prendere in considerazione il contenuto e il tono: infatti certe espressioni di odio sono più estreme, utilizzano termini più insultanti e possono perfino istigare altri ad agire. All'altra estremità della scala, troviamo insulti più moderati o generalizzazioni eccessive, che presentano certi gruppi o individui sotto una cattiva (e perfino sotto falsa) luce.

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?

In particolare nell'ultimo ciclo della scuola primaria e durante la scuola secondaria saranno individuate modalità per affrontare e prevenire la dipendenza da gioco online attraverso:

- **seminario teatrale promosso dall'ente comunale;**

- **giochi di ruolo per far sperimentare direttamente i rischi di un prolungato utilizzo di questi giochi;**

- **contenuti disciplinari riguardanti le probabilità di vincita e i meccanismi psicologici di rinforzo al gioco e di percezione della vincita/perdita.**

4.5 - Sexting

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

Il sexting (abbreviazione di sex – sesso e texting – messaggiare, inviare messaggi) indica l'invio e/o la ricezione di contenuti (video o immagini) sessualmente espliciti che ritraggono se stessi o gli altri.

"Spesso sono realizzate con il telefonino, e vengono diffuse attraverso il cellulare (tramite invio di mms o condivisione tramite bluetooth) o attraverso siti, e-mail, chat. Spesso tali immagini o video, anche se inviate ad una stretta cerchia di persone, si diffondono in modo incontrollabile e possono creare seri problemi, sia personali che legali, alla persona ritratta. L'invio di foto che ritraggono minorenni al di sotto dei 18 anni in pose sessualmente esplicite configura, infatti, il reato di distribuzione di materiale pedopornografico".

I contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di "revenge porn" letteralmente "vendetta porno" fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte. Tutto ciò è penalmente perseguibile dalla legge del 19 luglio 2019 n. 69, all'articolo 10 che ha introdotto in Italia il reato di revenge porn, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti.

La consapevolezza, o comunque la sola idea di diffusione di contenuti personali, si replica nel tempo e può finire con il danneggiare, sia in termini psicologici che sociali, sia il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che hanno contribuito a diffonderla. Due agiti, quindi, che sono fra loro strettamente legati e che rappresentano

veri e propri comportamenti criminali i quali hanno ripercussioni negative sulla vittima in termini di autostima, di credibilità, di reputazione sociale off e on line. A ciò si associano altri comportamenti a rischio, di tipo sessuale ma anche riferibili ad abuso di sostanze o di alcool.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/i e depressione: gli alunni devono diventare completamente consapevoli delle gravi conseguenze in caso di pratica del sexting attraverso interventi nella scuola sec. di primo grado mirati alla spiegazione e alle riflessioni guidate con loro su questo specifico tema.

4.6 - Adescamento online

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

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

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

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

Il nostro Istituto intraprende, per prevenire ed affrontare la delicata problematica dell'adescamento, lezioni di cyberbullismo sulle classi prime della sc. sec. di primo grado affrontando questo tema all'interno di questi approfondimenti.

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.

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 coinvolte/i 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.

La pedopornografia esiste da prima dell'avvento di Internet. Tuttavia, la diffusione della Rete, l'evoluzione e la moltiplicazione dei "luoghi" virtuali, il cambiamento costante delle stesse tecnologie digitali, ha radicalmente cambiato il modo in cui il materiale pedopornografico viene prodotto e diffuso, contribuendo ad un aumento della sua disponibilità e dei canali di diffusione. La diffusione della banda larga, ad esempio, consente di caricare e scaricare velocemente video e foto anche di grandi dimensioni, così come la diffusione delle videocamere e dei cellulari con videocamera incorporata, consente la produzione "in house" di materiale video, riproducibile facilmente online.

Secondo l'ultimo Rapporto annuale di INHOPE, relativo al 2018, il 91% delle immagini e video segnalate e risultate illegali, coinvolgeva bambini e bambine al di sotto di 13 anni; l'80% delle vittime era costituito da bambine e ragazze; l'84% del materiale risulta ospitato su servizi di image hosting (INHOPE è un network internazionale di 47 hotlines in 43 Paesi, cui aderisce anche "STOP-IT" di Save the Children e "Clicca e segnala" di Telefono Azzurro).

Sul versante nazionale, secondo i dati ISTAT più recenti, nel 2015 sono state avviate 1.032 indagini per il reato di atti sessuali con minorenni, nonché 720 per pornografia minorile.

Il nostro Istituto intraprende per prevenire ed affrontare la delicata problematica di pedopornografia lezioni di cyberbullismo sulle classi prime della sc. sec. di primo grado.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni:

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

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

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

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

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

☐ Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

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

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

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

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

Scegliere almeno 1 di queste azioni:

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

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

coinvolgimento di esperti.

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

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

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

☐ Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

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

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

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

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.

Il docente, qualora avesse il sospetto o la certezza di una situazione di cyberbullismo, sexting o adescamento online DEVE segnalarlo tempestivamente tramite procedure definite (in fondo a questo capitolo), che forniscono anche le indicazioni dei professionisti

e delle organizzazioni esterne che operano con la scuola. 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 se online , per quanto possibile, e il blocco della sua diffusione via dispositivi mobili.**

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.

Studenti e studentesse hanno a disposizione i seguenti strumenti:

- **sportello di ascolto con professionisti (per appuntamenti per la scuola primaria contattare l'Assistente Amministrativa Rita Muraca tel. 0522/857593, e-mail: rita.muraca@icspallanzani.org. Per la scuola media contattare la prof.ssa Federica Bassi, tel.0522/989554, e-mail: federica.bassi@icspallanzani.org).**
- **docente referente per le segnalazioni (Prof. Dallari Lara, tel. 0522/989554, e-mail: lara.dallari@icspallanzani.org).**

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.

Ci si può inoltre rivolgere ai seguenti servizi:

- **Helpline di Generazioni Connesse (numero verde: 19696) e Chat di Telefono Azzurro per supporto ed emergenze;**
- **Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online**

5.3. - 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.

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 esulino dalle competenze e possibilità della scuola. Ne elenchiamo di seguito alcuni presenti nella nostra regione.

SPORTELLO SOCIALE DI SCANDIANO

Indirizzo: via Reverberi 1, al secondo piano

tel.: 0522985860 e 0522985866 dal lunedì al sabato, fra le 7,30 e le 9,30

Ricevimento al pubblico:

martedì, giovedì e venerdì dalle 9,30 e le 13,00

lunedì, mercoledì e sabato CHIUSO

AZIENDE SANITARIE LOCALI

I riferimenti per contattare le aziende sanitarie della propria città si trovano al seguente l i n k :
http://salute.regione.emilia-romagna.it/ssr/aziende-sanitarie-irccs/erogazione-dellassistenza-aziende-sanitarieirccs-asp

Uffici Relazioni col pubblico distrettuali:

- **URP Arcispedale S. Maria Nuova - urp.santamarianuova@ausl.re.it**

(Tel. centralino: 0522.335111

- **URP Reggio Emilia - urp.reggioemilia@ausl.re.it**

- **URP Scandiano - urp.scandiano@ausl.re.it**

Le competenze erogate da questi servizi consistono nell'ottenere un sostegno psicologico, psichiatrico o neuropsichiatrico sulle problematiche psicologiche, anche associate all'uso di Internet e a tutti i tipi di comportamenti a rischio e che configurino un reato.

GARANTE REGIONALE PER L'INFANZIA E L'ADOLESCENZA

Viale Aldo Moro, 50 40127 Bologna, tel. 051. 5276263 - 051. 5275713

garanteinfanzia@regione.emilia-romagna.it

www.assemblea.emr.it/garanti/attivita-e-servizi/infanzia

Competenze/Servizi: Segnala all'autorità giudiziaria i servizi sociali e competenti; accoglie le segnalazioni di presunti abusi; fornisce informazioni sulle modalità di tutela e di esercizio di questi diritti; segnala alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate, sempre per tutti i comportamenti a rischio e che configurino un reato.

UFFICIO SCOLASTICO REGIONALE

Via de' Castagnoli, 1 40126 – Bologna. Tel: 051. 37851

direzione-emiliaromagna@istruzione.it

www.istruzioneer.it/

Competenze/Servizi: Tra le varie funzioni, supporta la scuola in attività di prevenzione. Può affiancare le scuole nei casi di segnalazione di comportamenti a rischio correlati all'uso di internet e per i comportamenti a rischio e che configurino un reato relativi al cyberbullismo.

TRIBUNALE PER I MINORENNI

Via del Pratello , 36 40122 – Bologna. Tel: 051. 2964880

tribmin.bologna@giustizia.it

http://www.tribmin.bologna.giustizia.it/

Competenze/Servizi: Tra le varie attività si occupa di tutti i procedimenti che riguardano reati, misure rieducative, tutela e assistenza, sempre per tutti i comportamenti a rischio e che configurino un reato.

POLIZIA POSTALE E DELLE COMUNICAZIONI

Via Francesco Zanardi, 28/6 – Bologna. Tel: 051. 6352611

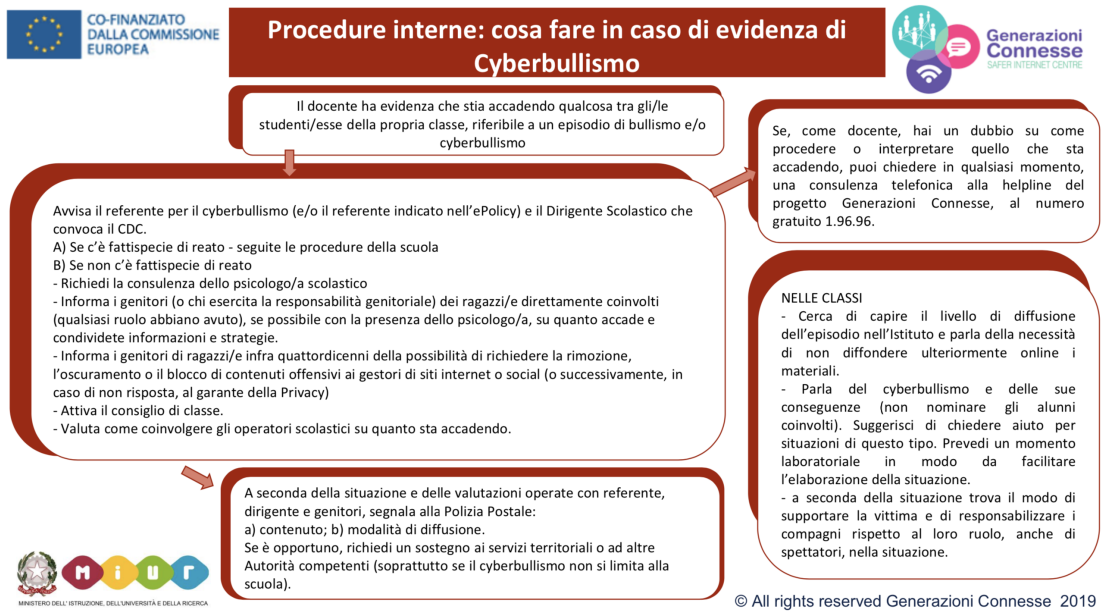
poltel.bo@poliziadistato.it

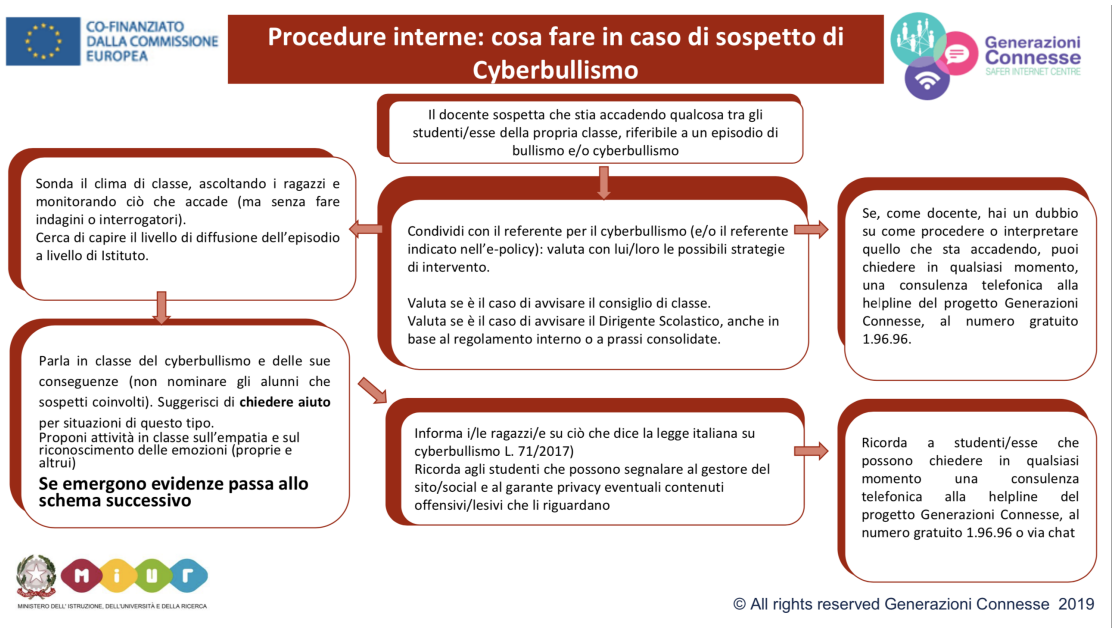
www.commissariatodips.it/

Competenze/Servizi: Si occupa di accogliere tutte le segnalazioni o denunce relative a comportamenti a rischio nell'utilizzo di internet sempre per tutti i comportamenti a rischio e che configurino un reato, quali: furto di identità, cyberbullismo (nel caso di cyberstalking), commercio on-line (nel caso di clonazione di carta di credito), pedopornografia on-line, grooming (adescamento on-line), gioco d'azzardo on-line, sexting.

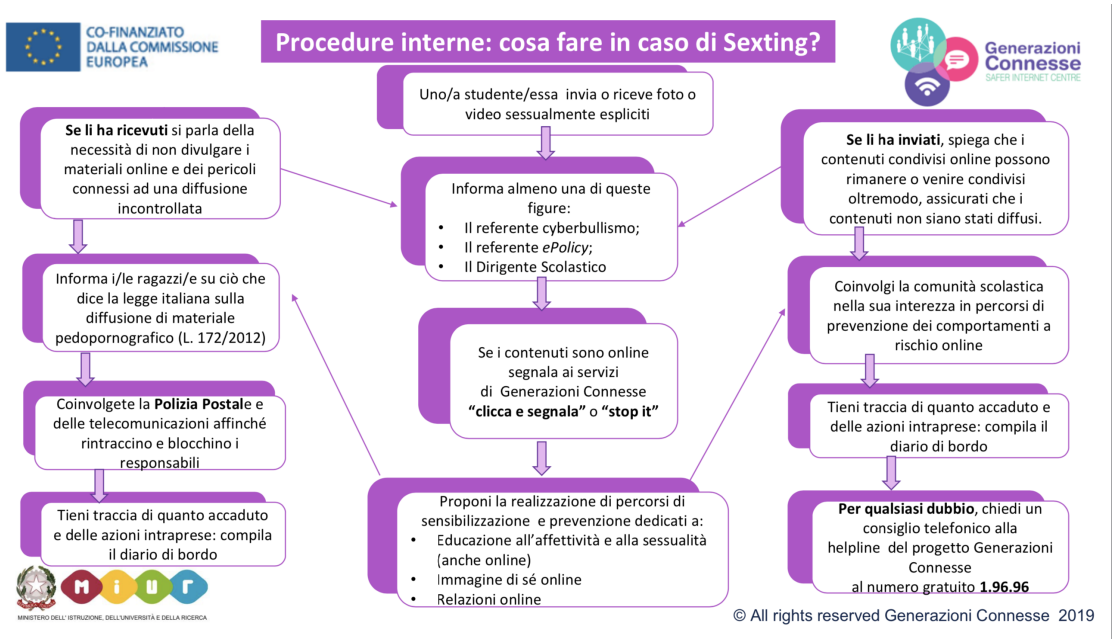
5.4. - Allegati con le procedure

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

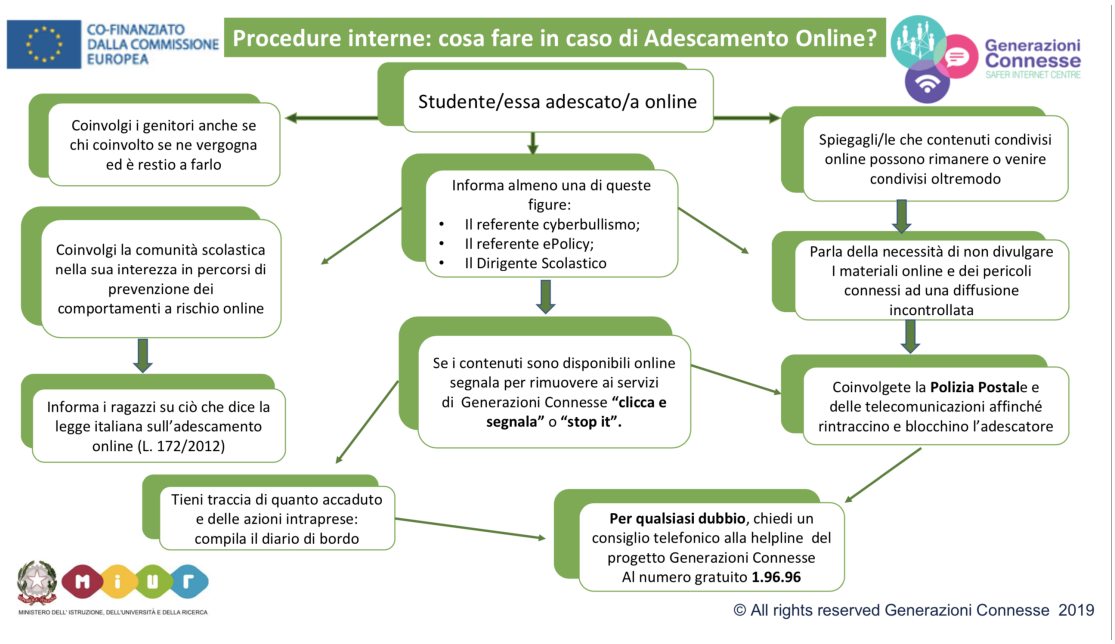




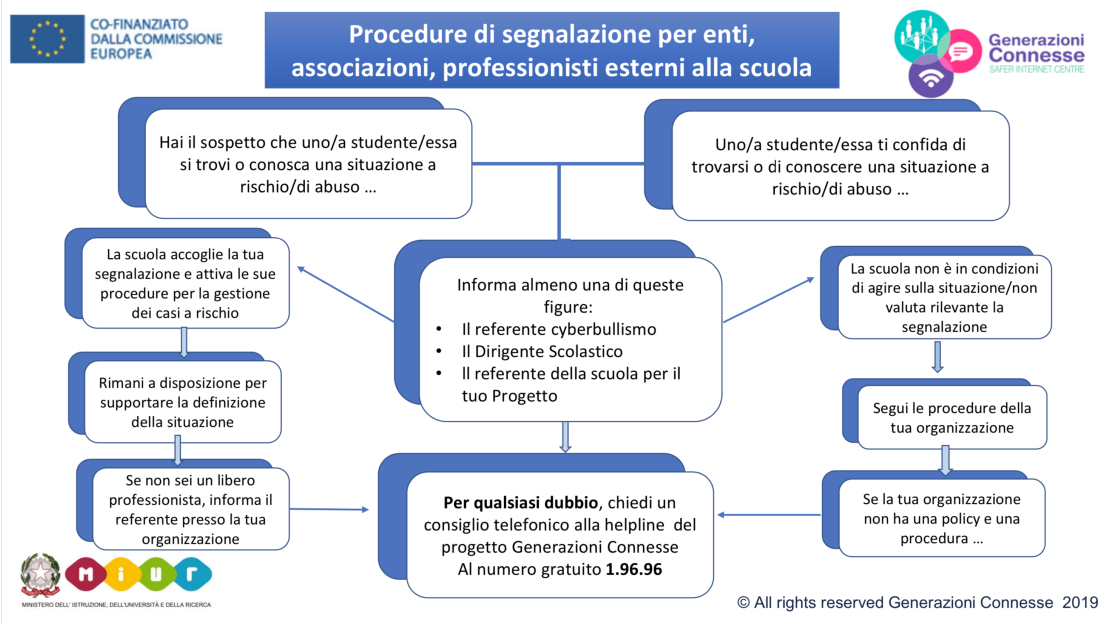
Procedure interne: cosa fare in caso di sexting?



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 INTERNE: COSA FARE IN CASO DI EVIDENZA DI CYBERBULLISMO E BULLISMO

Docente ha evidenza che stia accadendo nella propria classe un episodio di cyberbullismo

Avvisa il referente per il cyberbullismo (Prof. Dallari Lara, tel. 0522/989554, e-mail: lara.dallari@icspallanzani.org) e il Dirigente Scolastico che convoca il CDC.

1) Se c'è fattispecie di reato si seguono le procedure della scuola.	**2) Se non c'è fattispecie di reato:** **- richiedi la consulenza dello sportello psicologico;** **- informa i genitori per condividere informazioni e strategie;** **- informa i genitori di ragazzi/e infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet ;** **- valuta come coinvolgere gli operatori scolastici;** **- valuta se segnalare alla Polizia Postale o ad altri servizi territoriali;** **- se hai dei dubbi consulta l'helpline di Generazioni Connesse (19696) .**

PROCEDURE INTERNE: COSA FARE IN CASO DI SOSPETTO DI CYBERBULLISMO E BULLISMO

Il docente ha il sospetto che stia accadendo nella propria classe un episodio di cyberbullismo.

Avvisa il referente per il cyberbullismo (Prof. Dallari Lara, tel. 0522/989554, e-mail: lara.dallari@icspallanzani.org) e valuta con lui le strategie di intervento e se avvisare il CDC e il Dirigente Scolastico.

Monitora la situazione della classe e cerca di capire il livello di diffusione nell'Istituto.

Parla in classe del cyber bullismo, di ciò che dice la legge italiana (L. 71/2017), delle sue conseguenze e informa gli studenti che possono segnalare al gestore del sito internet o al garante della privacy eventuali contenuti offensivi/lesivi che li riguardano.

Se hai dei dubbi consulta l'helpline di Generazioni Connesse (19696) e ricorda agli studenti che possono farlo anche loro (anche tramite chat) .

PROCEDURE INTERNE: COSA FARE IN CASO DI SEXTING

Il docente viene a conoscenza che uno/a studente/essa invia o riceve foto o video sessualmente espliciti.

Informa il referente per il cyberbullismo (Prof. Dallari Lara, tel. 0522/989554, e-mail: lara.dallari@icspallanzani.org) e/o il Dirigente Scolastico.

Se i contenuti sono online segnala ai servizi di Generazioni Connesse “clicca e segnala” o “stop it” e parla della necessità di non divulgarli.

Se lo/a studente/essa li ha RICEVUTI, si contatta la Polizia Postale e delle telecomunicazioni affinchè rintraccino e blocchino i responsabili.

lnforma i/le ragazzi/e su ciò che dice la legge italiana sulla diffusione di materiale pedopornografico (L. 172/2012) e propone percorsi di sensibilizzazione e prevenzione.

Tieni traccia dell’accaduto e delle azioni intraprese.

Se hai dei dubbi consulta l’helpline di Generazioni Connesse (19696) .

PROCEDURE INTERNE: COSA FARE IN CASO DI ADESCAMENTO ONLINE

Il docente viene a conoscenza che uno/a studente/essa è stato/a adescato/a online.

Informa il referente per il cyberbullismo (Prof. Dallari Lara, tel. 0522/989554, e-mail: lara.dallari@icspallanzani.org) e/o il Dirigente Scolastico.

Se i contenuti sono online segnala ai servizi di Generazioni Connesse “clicca e segnala” o “stop it” per rimuoverli.

Coinvolgi i genitori e la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online.

Informa i/le ragazzi/e su ciò che dice la legge italiana sull’adescamento online (L. 172/2012) e spiega che i contenuti condivisi online possono rimanere o venire condivisi e dei pericoli connessi a una diffusione incontrollata.

Contatta la Polizia Postale e delle telecomunicazioni affinché rintraccino e blocchino gli adescatori.

Tieni traccia dell’accaduto e delle azioni intraprese.

Se hai dei dubbi consulta l’helpline di Generazioni Connesse (19696) .

Il nostro piano d'azioni

Non è prevista nessuna azione.