Documento di ePolicy

MEIS03400B

BARCELLONA MEDI

VIA DEGLI STUDI 74 - 98051 - BARCELLONA POZZO DI GOTTO - MESSINA (ME)

Domenica Pipitò

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'Istituto di Istruzione Superiore Liceo Medi ha elaborato questo documento in conformità alle "Linee di orientamento per azioni di contrasto al bullismo e cyberbullismo" del 15 Aprile 2015 e alla

successiva Nota del MIUR "Linee di orientamento per la prevenzione del bullismo e del Cyberbullismo" (ottobre 2017) e con la guida del Corso di Formazione all'interno del sito di Generazioni Connesse, al fine di educare e sensibilizzare l'intera comunità scolastica all'uso consapevole delle Nuove Tecnologie. La crescente diffusione delle TIC sia in ambito didattico, specie durante la DAD (Didattica a Distanza) e DDI (Didattica Integrata) sia nella vita quotidiana richiede infatti una maggiore responsabilità e consapevolezza affinchè tutti gli attori scolastici, discenti, docenti, personale non docente e genitori, possano utilizzare le Nuove Tecnologie in modo appropriato e sicuro. Di qui la necessità di dotare la scuola di una propria Policy di e-safety.

1.2 - Ruoli e responsabilità

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

Il Dirigente Scolastico deve: - garantire la corretta formazione del personale scolastico sulle tematiche relative all'uso sicuro e consapevole di Internet e della rete; - garantire una formazione adeguata del personale docente relativo all'uso delle TIC nella didattica; - garantire che le modalità di utilizzo corretto e sicuro delle TIC e di Internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi; - garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line; - seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola. L'Animatore digitale, supportato dal Team dell'innovazione, deve: - stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi; - monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da Documento di e-policy - redatto con il supporto del Safer Internet Centre - - assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione); - coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti alla "scuola digitale". Il referente del bullismo e cyberbullismo deve: - coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e cyberbullismo (può avvalersi della collaborazione delle Forze di polizia, Associazioni e centri di aggregazione giovanile del terrotorio). - coinvolgere (ove possibile), con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.

Il Direttore dei servizi generali e amministrativi deve: - assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia

funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni; - garantire il funzionamento dei diversi canali di comunicazione della scuola (circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di Internet. I Docenti devono: - informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di Internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento; - garantire che le modalità di utilizzo corretto e sicuro delle TIC e di Internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi; - garantire che gli alunni comprendano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di Internet; - assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete, ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore; - garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali; - assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente; - controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito); - nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei; - comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo; - segnalare qualsiasi problema o proposta di carattere informativo all'Animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC; - segnalare al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di Internet, per l'adozione delle procedure previste dalle norme. Gli Alunni devono: - essere responsabili, in relazione al proprio grado di maturità e di apprendimento, nell'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti; - avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali, ma anche della necessità di evitare il plagio e rispettare i diritti d'autore; - comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi; - adottare condotte rispettose degli altri anche quando si comunica in rete; - esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di Internet ai docenti e ai genitori. I Genitori devono: - sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle TIC nella didattica; - seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti; - relazionarsi in modo costruttivo con le docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i figli non usano responsabilmente le tecnologie digitali o Internet; - fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di Internet e dello smartphone in generale; - accettare e condividere quanto scritto nell'e-policy dell'Istituto. Infine, gli Enti esterni e le Associazioni devono: - conformarsi alla politica della scuola riguardo l'uso consapevole delle TIC e della Rete; - promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti durante le attività che si svolgono insieme.

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

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

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

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

> Organizzazioni/enti/associazioni extrascolastiche e gli esperti esterni chiamati, a vario titolo, ad intervenire nella realizzazione di progetti ed attività educative, sul breve o/e lungo periodo, dovranno prendere atto di quanto stilato nell' E-policy dell'Istituto e adeguarsi alle decisioni assunte e codificate all’interno del documento.

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

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

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

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

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

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

> L'e- Policy è un documento condiviso dall'intera comunità scolastica: ALUNNI: - potranno usare Internet e i dispositivi digitali solo sotto controllo dei docenti previa loro autorizzazione; - saranno adeguatamente informati riguardo all'uso responsabile e sicuro di Internet prima ancora di poter usare la rete; - prenderanno visione dell'elenco delle regole per la sicurezza on-line che sarà pubblicato sia sul sito della scuola sia all'interno dei laboratori multimediali; - saranno informati sulla e-safety ed i rischi online dai loro docenti e dalle iniziative della scuola . DOCENTI: - La politica di e-safety della scuola sarà discussa all'interno degli organi collegiali (consigli di classe, collegio dei docenti, dipartimenti disciplinari) e comunicata formalmente a tutto il personale della scuola tramite il sito web; - un'adeguata formazione del personale docente sull'uso sicuro e responsabile di Internet sarà assicurata attraverso corsi ed eventi online ed in presenza; - l'Animatore digitale pubblicherà sul sito della scuola un vademecum per la sicurezza sia per l'immediata consultazione sia per informare gli alunni. - GENITORI: - saranno adeguatamente informati sull'e-policy tramite comunicazioni e materiali pubblicati del sito web della scuola; - saranno coinvolti in eventi di formazione e dibattiti in materia di e-safety in occasione di celebrazioni (il SID) , degli incontri scuola-famiglia e delle assemblee collegiali e individuali; - l'Animatore digitale fornirà ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di Internet anche nella propria area domestica oltre a indirizzi sul web relativi a risorse utili per lo studio e a siti educativi per gli alunni.

1.5 - Gestione delle infrazioni alla ePolicy

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

Le possibili infrazioni in cui gli alunni potrebbero incorrere a scuola nell'utilizzo delle tecnologie digitali sono le seguenti: - uso improprio della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare; - trasmissione incauta o senza permesso di video o foto o di dati sensibili; - la condivisione di immagini intime; - la comunicazione incauta e senza permesso con sconosciuti; - il collegamento a siti web non indicati dai docenti. Sono previsti pertanto da parte dei docenti provvedimenti "disciplinari" proporzionati alla gravità del comportamento, quali: - il richiamo verbale; - nota disciplinare sul registro elettronico; - la convocazione dei genitori da parte degli insegnanti; - la convocazione dei genitori da parte del Dirigente scolastico. Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di re-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti d'amicizia e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni. 2) Disciplina del personale scolastico. Le possibili infrazioni da parte del personale scolastico e in particolare dei docenti potrebbero essere : - un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei; - un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi; - una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi; - una mancata informazione preventiva degli alunni sull'uso corretto e responsabile delle tecnologie digitali e di Internet; - una mancata vigilanza dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili rischi; - interventi parziali o nulli nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale. Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a Internet, procedere alla eventuale rimozione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, pur conservandone una copia. Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti disciplinari . 3) Disciplina dei genitori. Sono tenuti a vigilare sui propri figli evitando di: -

concedere una piena autonomia nella navigazione in rete ;- ignorare la tematica della e-safety e dei rischi online – indagare in caso di chiusura e di isolamento e di cambio sensibile d'umore perché da intendersi come campanello d'allarme di un grave disagio. I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto. Il presente documento si integra pienamente con i Regolamenti Interni di Istituto, in particolare il Regolamento BYOD, il Patto di Corresponsabilità , il regolamento DAD, la Privacy Policy e l'Informativa alle famiglie. Il regolamento BYOD regola l'uso dei dispositivi mobili, tablet e smartphone all'interno delle aule per uso esclusivamente didattico , prevedendo provvedimenti disciplinari per chi viola tali norme e richiamando "l'attenzione degli alunni, dei docenti e delle famiglie sulle possibili conseguenze di eventuali riprese audio/video o fotografie effettuate all'interno degli ambienti scolastici, al di fuori dei casi consentiti, e successivamente diffuse con l'intento di ridicolizzare compagni o insegnanti o addirittura allo scopo di intraprendere azioni che sono spesso definite con il termine di cyberbullismo. Tali azioni possono configurare, nei casi più gravi, gli estremi di veri e propri reati". Nel Patto di corresponsabilità si ribadisce l'importanza della collaborazione sinergica tra le due Agenzie Educative, la scuola e la famiglia. Quest'ultima infatti " si impegna a: consultare periodicamente il sito dell'Istituto per visionare le comunicazioni della scuola; stimolare l'alunno alla partecipazione il più possibile autonoma e responsabile alle attività di didattica a distanza e allo svolgimento dei compiti assegnati rispettando le scadenze; controllare che siano rispettate tutte le norme vigenti a difesa della privacy; vigilare affinché i contenuti delle lezioni, loro eventuali registrazioni e il materiale on

line che sono postati ad uso didattico non vengano utilizzati in modo improprio. Nel caso in cui l'allievo diffonda informazioni riservate, permetta l'uso di account da parte di terzi, comunichi il link della videoconferenza Cisco Webex e/o il codice di accesso alla classe virtuale, usi in modo improprio la chat all'interno di Cisco Webex, videoregistra la lezione e la condivide con terze parti, sarà sottoposto a sanzione disciplinare".

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto. Il presente documento si integra pienamente con i Regolamenti Interni di Istituto, in particolare il Regolamento BYOD, il Patto di Corresponsabilità , il regolamento DAD, la Privacy Policy e l'Informativa alle famiglie. Il regolamento BYOD regola l'uso dei dispositivi mobili, tablet e smartphone all'interno delle aule per uso esclusivamente didattico , prevedendo provvedimenti disciplinari per chi viola tali norme e richiamando "l'attenzione degli alunni, dei docenti e delle famiglie sulle possibili conseguenze di eventuali riprese audio/video o fotografie effettuate all'interno degli ambienti scolastici, al di fuori dei casi consentiti, e successivamente diffuse con l'intento di ridicolizzare compagni o insegnanti o addirittura allo scopo di intraprendere azioni che sono spesso definite con il termine di cyberbullismo. Tali azioni possono configurare, nei casi più gravi, gli estremi di veri e propri reati". Nel Patto di corresponsabilità si ribadisce l'importanza della collaborazione sinergica tra le due Agenzie Educative, la scuola e la famiglia. Quest'ultima infatti " si impegna a: consultare periodicamente il sito dell'Istituto per visionare le comunicazioni della scuola; stimolare l'alunno alla partecipazione il più possibile autonoma e responsabile alle attività di didattica a distanza e allo svolgimento dei compiti assegnati rispettando le scadenze; controllare che siano rispettate tutte le norme vigenti a difesa della privacy; vigilare affinché i contenuti delle lezioni, loro eventuali registrazioni e il materiale on line che sono postati ad uso didattico non vengano utilizzati in modo improprio. Nel caso in cui l'allievo diffonda informazioni riservate, permetta l'uso di account da parte di terzi, comunichi il link della videoconferenza Cisco Webex e/o il codice di accesso alla classe virtuale, usi in modo improprio la chat all'interno di Cisco Webex, videoregistra la lezione e la condivide con terze parti, sarà sottoposto a sanzione disciplinare".

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 monitoraggio e l' eventuale aggiornamento del documento di e-policy saranno a cura del Dirigente Scolastico con la collaborazione dell'Animatore digitale, del Team e del referente del bullismo e cyberbullismo. Il monitoraggio avrà il fine di rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di Internet. Il monitoraggio on-line sarà rivolto anche ai docenti al fine di valutare l'impatto della Policy e la necessità di eventuali miglioramenti.

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.

> L'IIS Medi ha già posto al centro del curricolo il raggiungimento della competenza digitale sia per i docenti che per gli studenti. A tale scopo non solo è sede per gli esami di ECDL per docenti ed alunni interni ed esterni all'istituzione scolastica ma è anche scuola polo per la formazione in provincia di Messina e pertanto eroga corsi di formazione (in presenza ed online) per i docenti sulla didattica per competenze e sull'uso delle nuove tecnologie all'interno del Piano Nazionale Scuola Digitale. L'Istituto ha inoltre aderito negli anni precedenti al progetto regionale " I peersbullo", in rete con 40 scuole della Sicilia, per prevenire e contrastare il fenomeno del bullismo e del cyberbullismo attraverso la Peer Education. Il Piano di Miglioramento prevede per l'Istituto, entro il prossimo triennio, l'attivazione di un Laboratorio per il coding e la robotica, integrando così le competenze digitali già previste dalle Indicazioni Nazionali, con la promozione dello sviluppo del "pensiero computazionale" negli alunni. Attività di sensibilizzazione sull'uso corretto delle tecnologie digitali con l'ausilio di esperti interni ed esterni (avvocati, psicologi, pedagogisti, ispettori di

Polizia) vengono annualmente organizzate in coincidenza con la giornata del Safer Internet Day (nel mese di febbraio) tramite la visione di film e documentari su tematiche inerenti al bullismo ed al cyberbullismo e conseguente dibattito tra gli alunni.

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.

Considerato che la formazione docenti è obbligatoria, come recita il comma 124 della Legge n. 107/2015 : "Nell'ambito degli adempimenti connessi alla funzione docente, la formazione in servizio dei docenti di ruolo è obbligatoria, permanente e strutturale. Le attività di formazione sono definite dalle singole istituzioni scolastiche in coerenza con il piano triennale dell'offerta formativa e con i risultati emersi dai piani di miglioramento delle istituzioni scolastiche", il corpo docente ha partecipato a corsi di formazione anche nell'ambito di Piani Nazionali e ad iniziative organizzate dall'Istituzione e possiede generalmente una buona competenza di base e, nel caso di alcune figure (Animatore digitale e Team dell'innovazione didattica), anche di carattere tecnico. I docenti sono inoltre aperti all'aggiornamento continuo (lifelong learning) dato il progresso galoppante delle nuove tecnologie. Perciò sono previsti percorsi individuali di autoaggiornamento , momenti di formazione collettiva anche all'interno dell'Istituto, con il supporto dell'Animatore digitale che quotidianamente aggiorna il sito della scuola con manuali, guide e tutorial per la didattica a distanza sull'uso delle TIC. Occasione di sviluppo professionale online è inoltre assicurata dalla piattaforma eTwinning, essendo l'IIS Medi "scuola eTwinning" ed essendo stata premiata anche con certificazioni europee (European Quality Label) per i risultati raggiunti all'interno di progetti eTwinning con partner europei specie sull'uso delle Nuove Tecnologie.

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.

> L'IIS Medi si avvale della figura dell'Animatore digitale che, con il Dirigente Scolastico e il D.S.G.A., collabora per raggiungere gli obiettivi di innovazione del PNSD nella scuola. Inoltre, a partire dall'anno scolastico 2017-2018 è attiva la figura del Referente d'Istituto per le attività di prevenzione e contrasto al bullismo e al cyberbullismo (L.107/2015). Si rende, comunque, necessaria la formazione di tutti i docenti sull'uso consapevole e sicuro di Internet e sui rischi della rete. Di conseguenza si prevedono per il futuro oltre ai momenti di formazione individuale e/ o collettiva, anche l'avvio di seminari, conferenze e dibattiti in presenza ed online con il supporto di esperti del territorio. Eventi di sensibilizzazione ed informazione saranno organizzati anche per gli alunni e le famigliein cooperazione con l'Amministrazione Comunale, i servizi socio-educativi e le associazioni del territorio.

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.

Scuola e famiglia collaborano in sinergia per garantire la crescita formativa di ciascun alunno. Non a caso all'inizio dell'anno scolastico viene stipulato il Patto Educativo di Corresponsabilità. Alla luce di tale collaborazione, l'Istituto attiverà iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e metterle in guarda di fronte alle insidie della rete. A tal fine saranno previsti incontri, dibattiti e seminari fra docenti e/o esperti e genitori sui temi oggetto della e-Policy. Contemporaneamente sul sito della scuola, inoltre, sarà pubblicato sia il documento di e-policy per la diffusione e condivisione di informazioni e procedure sia le risorse (materiali) per informare le famiglie sull'utilizzo delle nuove tecnologie all'interno dell'Istituto e prevenire i rischi legati ad un uso non corretto di Internet.

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.

In base al Decreto Legislativo del 30 giugno 2003, n.196 (Codice della Privacy), integrato dal D. Lgs. 10 agosto 2018, n. 101, e dal GDPR (General Data Protection Regulation) n. 679 del 2016, all'atto dell'iscrizione viene fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali dei propri figli. Nella fattispecie potranno essere utilizzate fotografie, video o altri materiali audiovisivi contenenti l'immagine e/o il nome degli alunni esclusivamente all'interno di attività educative e didattiche per scopi di documentazione, formazione e disseminazione. In particolare le immagini ed i video potranno essere pubblicati sul sito istituzionale (dominio edu.it) della scuola per documentare e divulgare attività specifiche e, previa autorizzazione dei genitori, anche su testate giornalistiche (locali e nazionali), giornalini d'Istituto e piattaforme Social come Facebook ed Instagram. L'autorizzazione non consente l'uso dell'immagine in contesti che pregiudichino la propria dignità personale ed il decoro e, comunque, per uso e/o fini diversi da quelli sopra indicati. In caso di partecipazioni a concorsi o manifestazioni, l'Istituto richiede apposita autorizzazione. Per la partecipazione, inoltre, alle attività dei Progetti Erasmus ed eTwinning della scuola viene richiesta un'ulteriore autorizzazione alle famiglie per la tutela della Privacy dei propri figli, in quanto la fase della disseminazione nazionale ed europea di tali progetti può prevedere la pubblicazione di foto e video su piattaforme europee, canali YouTube, riviste e giornali su scala nazionale ed internazionale. Fermo restando che il genitore, come si legge nel documento sulla tutela della Privacy pubblicato sul sito della scuola, "può sempre negare il proprio consenso o revocarlo in qualsiasi momento".. In base al Decreto Legislativo del 30 giugno 2003, n.196 (Codice della Privacy), integrato dal D. Lgs. 10 agosto 2018, n. 101, e dal GDPR (General Data Protection Regulation) n. 679 del 2016, all'atto dell'iscrizione viene fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali dei propri figli. Nella fattispecie potranno essere utilizzate fotografie, video o altri materiali audiovisivi contenenti l'immagine e/o il nome degli alunni esclusivamente all'interno di attività educative e didattiche per scopi di documentazione, formazione e disseminazione. In particolare le immagini ed i video potranno essere pubblicati sul sito istituzionale (dominio edu.it) della scuola per documentare e divulgare attività specifiche e, previa autorizzazione dei genitori, anche su testate giornalistiche (locali e nazionali), giornalini d'Istituto e piattaforme Social come Facebook ed Instagram. L'autorizzazione non consente l'uso dell'immagine in contesti che pregiudichino la propria dignità personale ed il decoro e, comunque, per uso e/o fini diversi da quelli sopra indicati. In caso di partecipazioni a concorsi o manifestazioni, l'Istituto richiede apposita autorizzazione. Per la partecipazione, inoltre, alle attività dei Progetti Erasmus ed eTwinning della scuola viene richiesta un'ulteriore autorizzazione alle famiglie per la tutela della Privacy dei propri figli, in quanto la fase della disseminazione nazionale ed europea di tali progetti può prevedere la pubblicazione di foto e video su piattaforme europee, canali YouTube, riviste e giornali su scala nazionale ed internazionale. Fermo restando che il genitore, come si legge nel documento sulla tutela della Privacy pubblicato sul sito

della scuola, “può sempre negare il proprio consenso o revocarlo in qualsiasi momento”.

3.2 - Accesso ad Internet

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

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

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

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

L’I.I.S. E. Medi garantisce l’accesso a Internet per fini didattici in tutti i plessi dell’Istituto, sia nelle aule, sia nei laboratori multimediali attraverso reti WiFi. La Dirigenza e l’Amministrazione hanno una rete separata. L'accesso ad Internet, attraverso i dispositivi della scuola da parte degli studenti, avviene solo in presenza dell'insegnante, il quale è responsabile del comportamento degli alunni nonché dei

dispositivi che utilizzano. È possibile effettuare installazioni e aggiornamenti di software solo tramite la password di amministratore, fornita al personale di assistenza tecnica. L'accesso all'homepage del sito della scuola non prevede password ma ovviamente servono le credenziali personali da parte dei docenti, degli studenti e dei genitori per accedere all'area riservata FAD (formazione a distanza, in cui sono presenti più di 500 classi virtuali) ed al registro elettronico. I computer presenti nelle aule e collegati direttamente alla LIM non richiedono una password di accesso per l'accensione . Dall'a.s. 2019/2020, causa pandemia Coronavirus, l'I.I.S. E. Medi ha acquistato le licenze Enterprise di Cisco Webex per consentire, a ciascun docente, di poter effettuare webinar/videoconferenze con gli studenti. La piattaforma, reperibile all'indirizzo https://ismedibarcellona.webex.com, consente, nel pieno rispetto della vigente normativa, lo svolgimento di riunioni degli organi collegiali in modalità telematica. A ciascun docente è stata assegnata una licenza individuale, con accesso, fornito dalla scuola, tramite alias del tipo nome.cognom@scuolamatica.net, dove il dominio scuolamatica.net è di proprietà del Medi. Tutte le pianificazioni delle riunioni avvengono tramiti protocolli comuni, sulla base di indicazioni fornite da tutorial realizzati dall'Animatore Digitale; i link e le password di accesso vengono condivisi esclusivamente nelle classi virtuali, permettendo un doppio tracciamento degli accessi mediante report emessi da Moodle e da Cisco Webex. I regolamenti DAD/DDI stabiliscono modalità tempi, strumenti e eventuali sanzioni (in caso di trasgressioni) riguardanti l'uso delle piattaforme.

3.3 - Strumenti di comunicazione online

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

Il sito dell'I.I.S. E. Medi è raggiungibile all'indirizzo https://www.liceomedi.edu.it (oppure www.liceomdi.it, con conseguente reinidirizzamento). La gestione del sito della scuola e la rispondenza alle normative per quanto concerne i contenuti in termini di accuratezza, appropriatezza ed aggiornamento, è a cura del Dirigente Scolastico e del Vicario (Animatore Digitale e Webmaster). Sul sito è possibile consultare il Regolamento d'Istituto e tutti gli altri Regolamenti (BYOD, DDI, AntiCovid, DAD etc.), la disseminazione di eventi e risultati finali di progetti didattici, avvisi alle famiglie, documentazione di attività curricolari ed extracurricolari in itinere o già concluse. È possibile accedere, tramite username e password individuali, all'area FAD (piattaforma Moodle) dove sono caricate, tra

l'altro, anche le comunicazioni interne di natura riservata. L'accesso a tale area è pertanto nominativo ed anche agli alunni vengono forniti username e password personali. Nella pubblicazione di contenuti sul sito della scuola è sempre posta attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative vigenti.

3.4 - Strumentazione personale

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

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

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

Il Regolamento BYOD dell'Istituto ribadisce la puntuale applicazione della normativa vigente (DPR 249/1998, DPR 235/2007, Direttiva Ministeriale 15.03.2007), riguardo l'uso degli smartphone/dispositivi digitali a scuola, in quanto non è consentito l'utilizzo come "cellulare" per ricevere/effettuare chiamate, SMS o altro tipo di messaggistica. Il divieto non si applica soltanto all'orario delle lezioni, ma è esteso anche agli intervalli e alle altre pause dell'attività didattica. Per quanto riguarda uscite, visite guidate e viaggi di istruzione, l'uso è consentito al di fuori dei momenti dedicati a visite guidate e attività prettamente didattiche. La comunicazione con le famiglie, per qualsiasi urgenza, è sempre garantita attraverso il telefono della scuola; i docenti possono derogare a tale disposizioni, consentendo l'uso del cellulare, in caso di particolari situazioni non risolvibili in altro modo. Le famiglie sono invitate a collaborare strettamente con l'Istituto, nello spirito della corresponsabilità educativa, evitando ad esempio di inviare messaggi o effettuare chiamate ai telefoni dei propri figli durante l'orario scolastico. Gli alunni sono tenuti a mantenere i loro telefoni spenti e riposti nello zaino durante l'intera permanenza a scuola. Possono usarli per scopi didattici solo su esplicita richiesta dei docenti per lo svolgimento di attività didattiche innovative e collaborative, che prevedano anche l'uso di dispositivi tecnologici e l'acquisizione

da parte degli alunni di un elevato livello di competenza digitale, soprattutto per quanto riguarda l'uso consapevole e responsabile delle tecnologie. Si ricorda che la competenza digitale è una delle competenze chiave per l'apprendimento permanente, identificate dall'Unione Europea. Secondo le recenti indicazioni del Garante della privacy, la registrazione delle lezioni è possibile, per usi strettamente personali. Qualora gli alunni intendessero avvalersi di tale possibilità, sono tenuti a informare l'insegnante prima di effettuare registrazioni audio/foto/video delle lezioni o di altre attività didattiche. In nessun caso le riprese potranno essere eseguite di nascosto, senza il consenso esplicito dell'insegnante. Si ribadisce che registrazioni e riprese audio/foto/video sono consentite per uso personale, mentre la diffusione di tali contenuti è invece sempre subordinata al consenso da parte delle persone ritratte/riprese. Si richiama l'attenzione degli alunni, dei docenti e delle famiglie sulle possibili conseguenze di eventuali riprese audio/video o fotografie effettuate all'interno degli ambienti scolastici, al di fuori dei casi consentiti, e successivamente diffuse con l'intento di ridicolizzare compagni o insegnanti o addirittura allo scopo di intraprendere azioni che sono spesso definite con il termine di cyberbullismo. Tali azioni possono configurare, nei casi più gravi, gli estremi di veri e propri reati. In generale, ogni utilizzo non autorizzato, al di fuori di quanto previsto in precedenza, non è permesso e sarà sanzionato. La scuola promuove iniziative di informazione e formazione sui temi dell'uso consapevole dei dispositivi informatici, dei nuovi media, dei social network e in generale delle applicazioni web e mobili. Tali iniziative sono rivolte principalmente agli alunni ma anche, ove possibile, alle famiglie.

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.*

L'IIS Medi intende proseguire azioni di prevenzione e di sensibilizzazione in collaborazione con la rete dei servizi del territorio (Polizia postale, ASL, associazioni locali) allo scopo di educare gli allievi sia del biennio che del triennio ad un uso consapevole di Internet e metterli in guardia nei confronti dei pericoli della rete. Tale percorso di prevenzione coinvolgerà anche le famiglie. Al tempo stesso sarà avviata la formazione dei docenti. Tali iniziative saranno in presenza, alla fine dell'emergenza Covid-19, ma anche online mediante la creazione di webinar tramite la piattaforma Cisco Webex. Ogni anno, nel mese di febbraio, in occasione della celebrazione del Safer Internet Day, sarà creato un evento di sensibilizzazione e

prevenzione per la componente studenti, docenti e genitori.

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).

In riferimento alla problematica del cyberbullismo, l'IIS Medi potrà adottare piani di prevenzione a tre livelli: universale, selettiva e indicata . Nell'ambito della Prevenzione Universale, partendo dal presupposto che tutti gli studenti siano potenzialmente a rischio, saranno attuati interventi su larga scala, non limitati ad una o più classi ma all'intera popolazione studentesca dell'istituto. Dal punto di vista didattico si perseguirà l'obiettivo

della cittadinanza digitale in quasi tutte le discipline. Riguardo alla Prevenzione Selettiva, si interverrà, se fosse necessario, nei confronti di una classe o gruppo di studenti in cui il rischio online è presente. In questo caso la presenza del rischio è stata individuata tramite precedenti indagini e/o questionari, segnalazioni da parte degli alunni stessi o rivelazioni all'interno del Centro d'Ascolto. In tal caso gli interventi sono mirati e si pongono l'obiettivo di migliorare le competenze digitali e le strategie di problem solving. Infine, per quanto concerne la Prevenzione Indicata, si tratta di intervento sul caso specifico, con l'aiuto di esperti, per supportare l'eventuale vittima e redimere il cyberbullo.

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.

Per prevenire e contrastare fenomeni di "hate speech" da parte di singoli alunni o gruppi di alunni lo sviluppo delle competenze digitali e l'educazione ad un uso critico e consapevole delle nuove tecnologie assumono un ruolo centrale. Bisognerà allora offrire agli adolescenti gli strumenti necessari per abbattere gli stereotipi legati alla razza, al genere, all'orientamento sessuale e alla disabilità che si traducono in atteggiamenti verbali violenti diffusi attraverso la rete ed in particolare i social media. L'IIS Medi potrà avvalersi della collaborazione di esperti e consulenti esterni per organizzare

incontri formativi rivolti a docenti, alunni e genitori. Ma la formazione e l'educazione alla tolleranza, all'accettazione dell'altro ed alla partecipazione democratica del vivere in società potrà essere affrontata dai docenti all'interno dei propri curricula ed anche attraverso progetti trasversali, percorsi di PCTO e di Educazione Civica.

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?

A volte i nostri allievi manifestano "dipendenza da Internet": trascorrono così tante ore nella rete al punto da provare "astinenza" se costretti a distaccarsene. Lo stesso dicasi quando vengono travolti dalla frenesia del gioco online, che può degenerare in vera e propria patologia. In questi casi dovere della scuola è intervenire non per demonizzare la tecnologia o il gioco, ma per cercare di correggere comportamenti devianti che rischiano di annullare quanto di positivo può offrire la rete se adeguatamente utilizzata. L'intervento sarà proficuo se condiviso e supportato dalla famiglia, per stabilire mezzi e modalità durante lo studio domestico, con forme di controllo attivo durante la navigazione in Internet. L'Istituto si propone di promuovere un uso maggiormente consapevole delle tecnologie per favorire il "benessere digitale", ossia la capacità di sfruttare le opportunità offerte dai media digitali controllando le dinamiche indesiderate, l'impatto sulla salute, la gestione del tempo e dell'attenzione. Se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi. Gli interventi della scuola sul "benessere digitale" prenderanno in considerazione seminari, dibattiti, tavole rotonde, in presenza ed online, con la presenza di esperti esterni del territorio.

4.5 - Sexting

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti 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.

> Per prevenire rischi di sexting ovvero lo scambio di immagini audio e/o video a sfondo sessuale o sessualmente espliciti tramite smartphone e chat dei social media saranno attuate campagne di sensibilizzazione sia mediante il sito della scuola sia con interventi mirati in dibattiti/tavole rotonde con esperti (medici, psicologi, avvocati). Il sexting è un fenomeno comune tra gli adolescenti e rientra nel processo di costruzione e scoperta della propria identità; sono i mezzi utilizzati per la diffusione di tali immagini a generarne la pericolosità. Trasmesse tramite il web e i social networks rischiano di diventare virali e di sfuggire a qualsiasi controllo con gravi conseguenze per la vittima ritratta di natura sia legale sia emotiva. In tal caso il dialogo è essenziale così come la sensibilizzazione sulla natura delle piattaforme utilizzate e la consapevolezza dei rischi ad esse connesse. Qualora un caso di sexting dovesse verificarsi tra gli alunni dell'IIS Medi e venisse evidenziato in seguito a segnalazioni oppure all'interno del centro d'ascolto o riferito alla docente referente, la scuola contatterebbe immediatamente la Polizia Postale e delle Comunicazioni per la rimozione del materiale on line ed il blocco della sua diffusione tramite i dispositivi mobili.

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.

La problematica dell'adescamento online è da collocarsi in uno scenario più ampio di scarsa educazione emotiva, sessuale e di assenza di competenza digitale. Pertanto gli interventi di prevenzione vanno inseriti all'interno in un percorso di educazione digitale all'affettività e alla sessualità con l'ausilio di esperti (psicologi dell'età evolutiva, neuro-psichiatri). Seminari, dibattiti, tavole rotonde su questa tematica così delicata ed anche formazione sulle insidie che si nascondono nell'uso distorto delle nuove tecnologie sarebbero utili per sensibilizzare gli studenti e renderli emotivamente più sicuri e pronti ad affrontare eventuali situazioni a rischio, imparando a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. Le eventuali vittime non devono vergognarsi o o sentirsi in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Fondamentale quindi, è portare avanti un percorso di educazione digitale che includa i mezzi per proteggere la propria privacy e gestire l'immagine e l'identità online. Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere all'adescatore. È importante che il computer o altri dispositivi elettronici non vengano usati per non compromettere eventuali prove e che i contenuti non vengano rimossi. Casi di adescamento online richiedono l'intervento della Polizia Postale e delle Comunicazioni a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore. Per quanto concerne la vittima occorrerà l'azione congiunta della famiglia e dei servizi del territorio (Consultorio Familiare, Servizio di Neuropsichiatria infantile) per evitare ripercussioni psicologiche significative sul minore.

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 è un reato e spesso strettamente connessa a sexting e grooming. L'IIS Medi tratterà anche queste tematiche in campagne di prevenzione e sensibilizzazione annuali all'interno della scuola coinvolgendo alunni, docenti e genitori. Qualora venisse segnalato un caso di pedopornografia ai danni di allievo/a dell'Istituto, si procederà immediatamente ad avvisare le autorità competenti (Polizia di Stato, Questura o Commissariato del territorio, Arma dei Carabinieri) al fine di rimuovere il materiale dalla rete e per identificare il colpevole.
> Parallelamente, per salvaguardare il benessere psicofisico degli alunni coinvolti nella visione di questi contenuti, sarà opportuno ricorrere a un supporto psicologico anche passando per una consultazione presso il medico di base o pediatra di riferimento. Le strutture pubbliche a cui rivolgersi sono i servizi socio-sanitari del territorio di appartenenza: Consultori Familiari, Servizi di Neuropsichiatria infantile, centri specializzati sull'abuso e il maltrattamento all'infanzia, etc

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 ai genitori e ai docenti, con il coinvolgimento di esperti.

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

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 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.

Le procedure d'intervento saranno condivise con l'intera comunità scolastica e saranno visibili sul sito della scuola (www.liceomedi.edu.it). Il docente referente, nominato dal Dirigente Scolastico all'inizio dell'anno scolastico, assumerà il coordinamento delle attività sia di prevenzione sia di intervento. Il Team operativo sarà costituito dalla DS, dall'Animatore Digitale, dalla referente Bullismo e

Cyberbullismo e dalla docente referente progetto Generazioni Connesse. Le docenti referenti (bullismo e cyberbullismo/Generazioni Connesse) sono le due figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso.Le procedure d'intervento saranno condivise con l'intera comunità scolastica e saranno visibili sul sito della scuola (www.liceomedi.edu.it). Il docente referente, nominato dal Dirigente Scolastico all'inizio dell'anno scolastico, assumerà il coordinamento delle attività sia di prevenzione sia di intervento. Il Team operativo sarà costituito dalla DS, dall'Animatore Digitale, dalla referente Bullismo e Cyberbullismo e dalla docente referente progetto Generazioni Connesse. Le docenti referenti (bullismo e cyberbullismo/Generazioni Connesse) sono le due figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso.

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.

Per quanto riguarda la gestione dei casi, l'IIS Medi ha individuato due figure referenti per il cyberbullismo che si occuperanno del coordinamento delle attività in tutti i plessi della scuola. La segnalazione del caso potrà essere avviata attraverso varie modalità: a) segnalazione da parte di un docente ; b) segnalazione da parte di un alunno tramite lo sportello d'ascolto; c) segnalazione tramite apposito indirizzo email; d) segnalazione anonima tramite scatola/box situata in area visibile nei locali scolastici dei singoli plessi. Dopo la segnalazione, il Team operativo attiverà i vari passaggi della procedura: indagini ed approfondimenti, raccolta informazioni, colloqui con gli attori coinvolti, coinvolgimento del DS , delle famiglie e del Consiglio di Classe. Se la gravità del caso lo richiede, ci si rivolgerà agli organi esterni (Polizia Postale o Servizi Sociali).

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

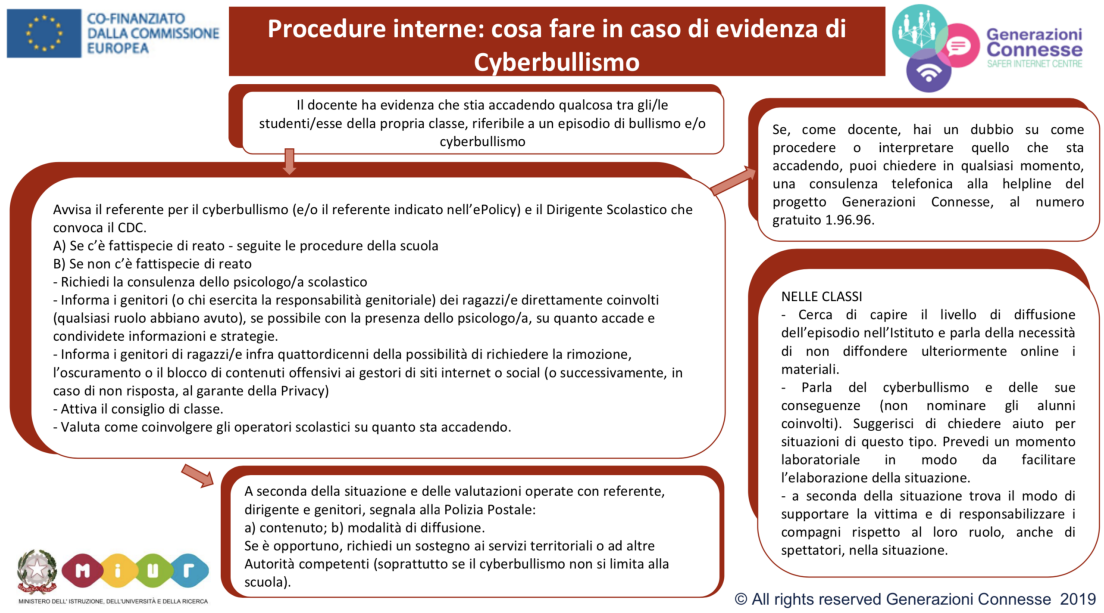
controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.

- **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.

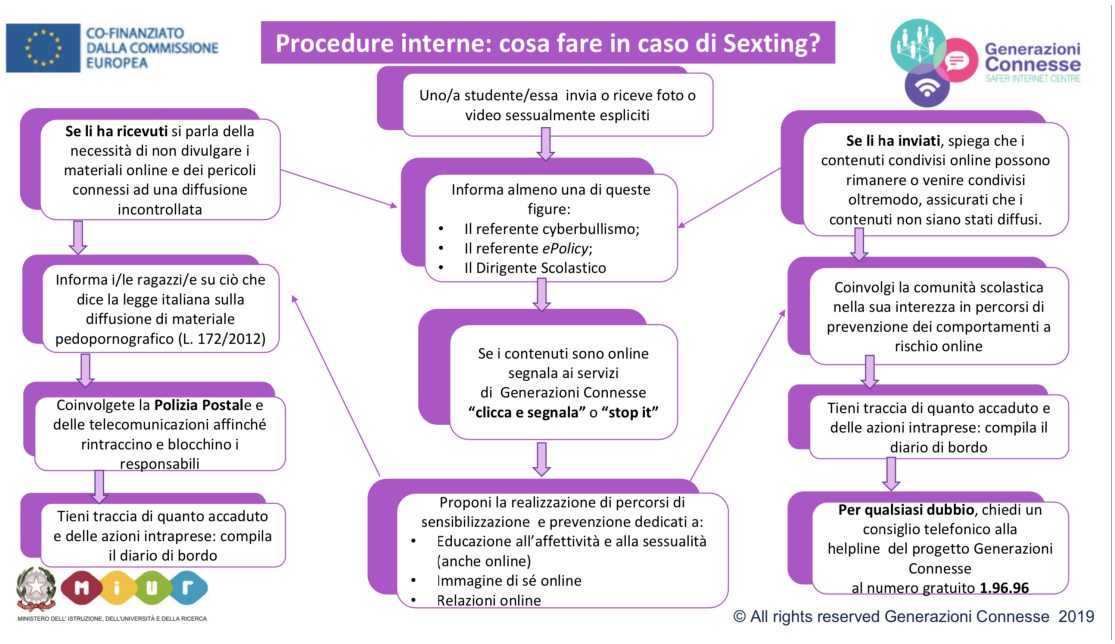
Nei casi di maggiore gravità l'IIS Medi chiederà l'intervento dei Servizi sul territorio e precisamente: l'Ufficio Scolastico Regionale di Palermo- sia come supporto per attività di prevenzione nelle scuole sia come intervento nei casi di segnalazione per reati connessi all'uso della rete, in particolare il cyberbullismo; il Tribunale per i minorenni di Messina- che si occupa di tutti i procedimenti che riguardano reati, misure rieducative, tutela ed assistenza; Polizia Postale e delle Comunicazioni di Catania o di Palermo- che accoglie tutte le segnalazioni o denunce relative a comportamenti a rischio nell'utilizzo di internet e che si configurano come reati : 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; l'Azienda Sanitaria locale- per ricevere sostegno psicologico, psichiatrico o neuropsichiatrico sulle problematiche psicologiche, anche associate all'uso di Internet.

5.4. - Allegati con le procedure

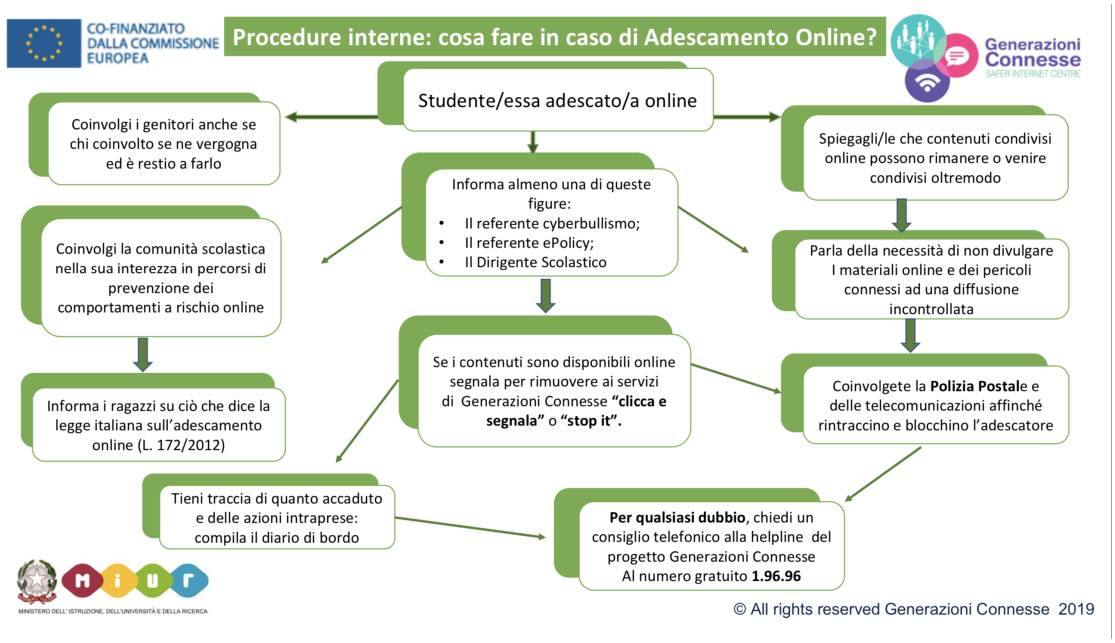
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



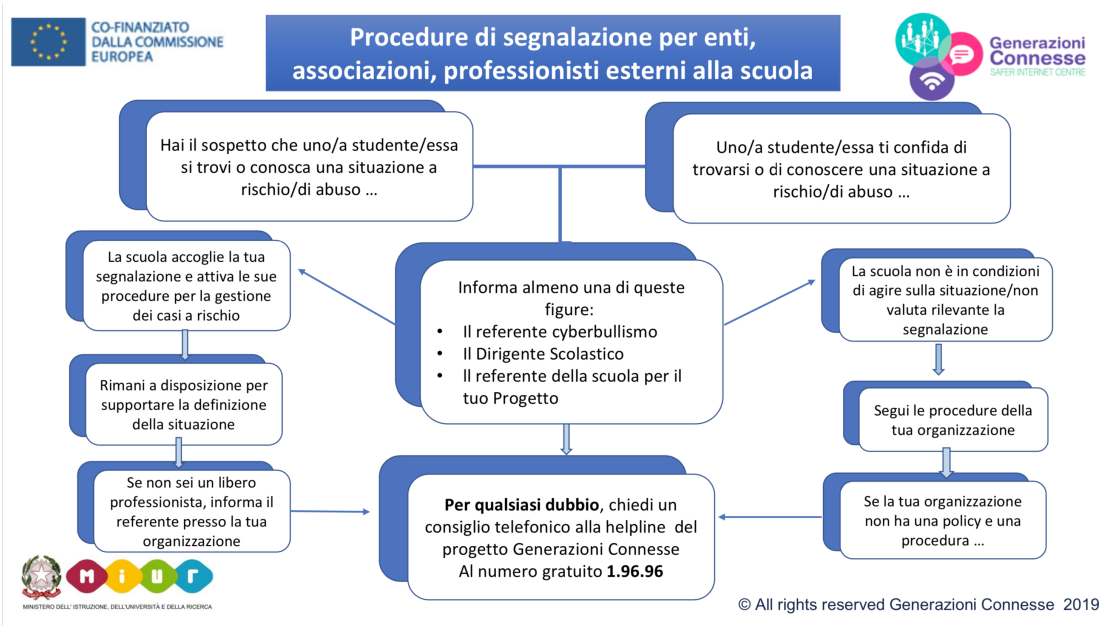
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

A seconda dei casi di sospetto o di evidenza si seguiranno le procedure come da protocollo (visualizzate nelle schede standard). Per le segnalazioni si utilizzerà la scheda allegata. inoltre il docente referente terrà aggiornato il Diario di Bordo.

Il nostro piano d'azioni

Eventi di prevenzione, sensibilizzazione ed informazione per alunni, docenti e genitori in presenza ed online