LICEO SCIENTIFICO STATALE - "G. BERTO"-VIBO VALENTIA
Prot. 0000470 del 30/01/2023
I-4 (Uscita)

Documento di ePolicy

VVPS01000R

LICEO SCIENTIFICO G.BERTO

C.DA BITONTO - 89900 - VIBO VALENTIA - VIBO VALENTIA (VV)

LICIA M. BEVILACQUA

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

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'impatto della tecnologia nella ordinarietà della nostra esistenza ha favorito l'interesse da parte della scuola in generale,, e del nostro Liceo in maniera particolare in merito allo sviluppo ed integrazione nella didattica e nelle attività educative a considerarne la sicurezza e la consapevolezza del suo utilizzo .In questi ultimi anni, il nostro Liceo si è confrontato con tematiche di questo tipo, organizzando eventi formativi in occasione del Safer Internet Day e partecipando a progetti organizzati da "Generazioni connesse". La redazione del presente documento nasce dalla necessità di dare concretezza alle
"Linee di orientamento" emanate nell'aprile 2015 tenendo conto, altresì, dei recenti interventi normativi e, in particolare, delle novità contenute nella L.71/2017 "Disposizioni a
tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo".Lo scopo che ci si propone in questa sede è, dunque, quello di descrivere l'approccio dell'istituto alle tematiche legate alle competenze digitali, all'uso degli stessi in ambiente
scolastico, ed alla sicurezza in rete in termini di:
- individuazione di norme comportamentali e delle procedure per l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC);
- promozione dell'uso positivo delle tecnologie digitali nella didattica;
- adozione delle misure per la prevenzione del fenomeno del cyberbullismo e, contestualmente, individuazione degli strumenti di tutela per chi risultasse vittima di comportamenti (anche solo potenzialmente) vessatori e di emarginazione
attraverso un uso distorto e violento della rete;
- sensibilizzazione degli studenti, orientandoli verso un uso corretto delle tecnologie digitali.
Il tutto in coerenza con lo spirito della Legge 71/2017 che è quello di un approccio sostanzialmente educativo ed inclusivo.
Il presente documento sarà soggetto a revisioni ed aggiornamenti annuali e
sottoposto all'attenzione dei competenti Organi Collegiali.

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.

1. Dirigente Scolastico

il Dirigente Scolastico è il garante per la sicurezza e la prevenzione di problematiche offline e online di tutti i membri della comunità scolastica, in linea con il quadro normativo di riferimento e le indicazioni del MIUR. Coadiuvato dal docente referente sulle tematiche del bullismo/cyberbullismo, promuove, avvalendosi del supporto degli enti locali, la cultura della sicurezza online. Organizza corsi di formazione specifici nonché attività di sensibilizzazione per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC. Inoltre, il Dirigente Scolastico ha la responsabilità di gestire ed intervenire nei casi di gravi episodi di bullismo, cyberbullismo ed uso improprio delle tecnologie digitali seguendo un protocollo che prevede le seguenti azioni:

accogliere le segnalazioni di eventi problematici relativi all'uso delle TIC o a eventi di bullismo/cyberbullismo

applicare la normativa specifica per la gestione dei casi segnalati

relazionarsi con gli enti preposti presenti sul territorio

garantire il funzionamento dei diversi canali di comunicazione della scuola (circolari,sito web) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti

2. Animatore Digitale

Coordina il Team digitale e organizza percorsi di formazione interna all'Istituto per il personale scolastico negli ambiti di sviluppo della "scuola digitale".

Supporta il personale scolastico da un punto di vista non solo tecnico-informatico oltre che essere uno dei promotori di percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale"

Collabora con i docenti e i tecnici responsabili dei laboratori per la stesura del Regolamento per l'uso responsabile delle TIC a scuola.

E' responsabile della creazione della piattaforma e-learning a scuola; fornisce credenziali di accesso, crea account per docenti e alunni, monitora il corretto funzionamento della piattaforma.

3. DSGA

Assicura, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per

garantire che l'infrastruttura tecnica della scuola sia funzionante e sicura ; garantisce il funzionamento dei diversi canali di comunicazione della scuola (circolari,sito web) 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.

4. Referente bullismo e cyberbullismo

L'Istituzione scolastica individua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo" (Art. 4 Legge n.71/2017, "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo").

Tale figura supporta il Dirigente scoalstico e coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo; collabora con le Forze di polizia e delle associazioni presenti sul territorio per prevenire e gestire i casi di CB; ove possibile coinvolge, con progetti e percorsi formativi, studenti, colleghi e genitori; promuove la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica ; applica e controlla i protocolli di rilevazione; monitora le potenziali azioni di CB; coinvolge la comunità scolastica nella partecipazione ad attvità e progetti relativi all'uso consapevole del web.

5. I Docenti

Si informano e si aggiornano sulle problematiche attinenti alla sicurezza nell'utilizzo delle TIC e sui Regolamenti adottati dalla scuola assicurandonr il rispetto.

Diffondono la cultura dell'uso responsabile delle TIC e della Rete. Integrano parti del curriculum della propria disciplina con approfondimenti promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica; segnalano al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti gli studenti al fine di approfondire e coordinare coerenti linee di intervento di carattere educativo; forniscono chiare indicazioni sul corretto utilizzo della rete condividendo con gli alunni la netiquette e indicandone le regole; leggono e sottoscrivono la presente e-policy

6. Il personale Amministrativo, Tecnico e Ausiliario (ATA)

Il personale ATA ciascuno per la propria funzione, svolge attività di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività della istituzione scolastica, in collaborazione con il dirigente scolastico e con il personale docente tutto; partecipa ad attività di formazione e autoformazione in tema di bullismo e cyberbullismo. Il personale ATA all'interno dei singoli regolamenti d'Istituto, è coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di

bullismo/cyberbullismo, insieme ad altre figure e nel raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo/cyberbullismo

7. Gli Studenti e le Studentesse

Gli Studenti e le Studentesse devono utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; avere comprensione delle potenzialità offerte dalle TIC per la ricerca di materiali sul Web evitando il plagio e rispettando il diritto di autore;

imparare a tutelarsi online, adottare condotte rispettose, tutelare i/le propri/e compagni/e ; partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete ; leggere comprendere e rispettare l'e_policy; capire l'importanza di segnalare abusi; capire la politica della scuola sull'uso di immagini e il CB; non utilizzare propri dispositivi senza avere acquisito il permesso dell'insegnante.

8. Genitori

In continuità con l'Istituto scolastico, si rendono partecipi e attivi nelle attività di promozione ed educazione sull'uso consapevole delle TIC e della Rete, nonché sull'uso responsabile dei device personali;

si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicano con loro circa i problemi rilevati quando i/le propri/e figli/e non usano responsabilmente le tecnologie digitali o Internet;

accettano e condividono quanto scritto nell'ePolicy dell'Istituto.

9. Gli Enti educativi esterni e le associazioni

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola devono conformarsi alla politica della stessa riguardo all'uso consapevole della Rete e delle TIC; dovono, inoltre, promuovere comportamenti sicuri, la sicurezza online e assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

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

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del

minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

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

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

La scuola si doterà di una informativa sintetica sull'ePolicy che condividerà con le organizzazioni/associazioni extrascolastiche ed esperti esterni impegnati nella realizzazione di progetti ed attività educative a breve /lungo periodo.

Verranno chiarite le stesse modalità di intervento e segnalazione per i professionisti, utili a rilevare e gestire le problematiche connesse ad un uso scorretto delle TIC .

L'informativa verrà condivisa e sottoscritta nella stipula di contratti con esperti e associazioni coinvolti in progetti e attività educative.

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

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

studenti/esse) si faccia a sua volta promotore del documento.

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

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

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

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

Il Liceo si impegna a diffondere la presente policy per condividerne i contenuti con tutta la comunità educante nei modi seguenti :

pubblicazione sul sito della scuola;

sottoscrizione del Patto di corresponsabilità da parte delle famiglie e dell'ePolicy;

- condivisione e comunicazione a studenti e studentesse (discussione in classe nei primi giorni di scuola condivisione di regole per un utilizzo corretto delle TIC, promozione di eventi formativi/informativi , rivolti ad alunni e genitori con il coinvolgimento di esperti , sui temi oggetto del codesto Documento);

- condivisione e comunicazione al personale scolastico (definizione di una linea di condotta di utilizzo accettabile , controllato e limitato alle esigenze didattiche;

- formazione/informazione del personale docente in presenza e online sull'uso responsabile e sicuro di internet;

- confronto collegiale , su base annuale , circa la necessità di apportare modifiche o migliorare il presente documento

- condivisione e comunicazione a genitori :

- sarà favorita la collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet ;

- saranno organizzati su richiesta , incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare.
I genitori verranno invitati a prestare la massima attenzione ai principi e alle regole

contenute nel presente documento. ;

Ciascun attore scolastico (dai docenti agli alunni) si farà a sua volta promotore del documento.

1.5 - Gestione delle infrazioni alla ePolicy

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

La comunità scolastica nel rispetto delle proprie funzioni rileverà le infrazioni alla policy ; alunni e genitori segnaleranno l'abuso secondo il seguente protocollo :

- Docenti o ATA ;

- Referente del cyberbullismo;

-Dirigente scolastico

La scuola prenderà tutte le precauzioni necessarie per garantire la sicurezza on-line; al personale e agli alunni saranno date informazioni sulle infrazioni in cui potrebbero incorrere e le conseguenti sanzioni contenute nel Regolamento di Istituto o nel presente documento. Nello specifico si potrà tener conto di quanto indicato nella seguente tabella

ALUNNI PERSONALE SCOLASTICO GENITORI

INFRAZIONI	Qualsiasi rilevazione di sospetto abuso, offesa, procurato disagio ricevuto su internet, sia personale che di un compagno Uso improprio del cellulare Atti di bullismo online Condivisione online di immagini o video di compagni/e senza il loro consenso o che li ritraggono in pose offensive e denigratorie; Condivisione di scatti intimi e a sfondo sessuale; la condivisione di dati personali; l'invio di immagini o video volti all'esclusione di compagni/e.	Condivisione di immagini/video che ritraggono docenti o personale scolastico nello svolgimento dell'attività scolastica Utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale Trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi Diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi Insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale	Piena autonomia concessa ai figli nella navigazione sul web Piena autonomia nell'utilizzo dello smartphone senza controllo/condivisione dei contenuti Inadeguata conoscenza che la responsabilità dei contenuti dei dispositivi utilizzati dai figli minori , sia ascrivibile ai genitori
AZIONI	DS, referente CB, ATA primo contatto per gestione dei casi ; organi competenti per casi più gravi configurati come vero e proprio reato	DS, Animatore digitale, referente CB, ATA per verificare l'utilizzo delle TIC in conformità alle regole di sicurezza. Avvio di procedimenti che possono avere carattere organizzativo,disciplinare, penale a seconda del tipo delle infrazioni commesse.	DS , referente CB convocano i genitori per condividere azioni educative o sanzionare a norma di legge in base alla gravita dei comportamenti dei propri figli

E' bene ricordare a tutti che nel momento in cui un qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia.

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 documento ePolicy è parte integrante del Regolamento di Istituto, Regolamento di disciplina e Patto di Corresponsabilità reperibili sul sito della scuola.

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.

Tutta la comunità scolastica è coinvolta nel monitoraggio dell'utilizzo di Internet, nell'applicazione delle istruzioni sull'uso sicuro e responsabile della Rete.
Il monitoraggio dell'implementazione della policy e del suo eventuale aggiornamento sarà svolto annualmente e/o qualora se ne ravvisasse la necessità. Tale monitoraggio sarà curato dal Dirigente scolastico con la collaborazione dell'Animatore digitale , dal referente del CB e dai docenti delle classi, tramite moduli di rilevazione ai fini della verifica della situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso responsabile del web (i parametri utili per il monitoraggio potrebbero riferirsi al numero delle segnalazioni, delle infrazioni, delle sanzioni disciplinari per ogni anno scolastico). Il monitoraggio sarà rivolto anche agli insegnanti, 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:

- Creazione del gruppo di lavoro ePolicy
- Realizzazione di un sistema di monitoraggio delle attività
- Realizzazione di un'assemblea per discutere delle attività di progetto

Azioni da svolgere nei prossimi 3 anni:

- Azione 1 Organizzare attività o eventi volti a presentare il progetto e consultare docenti e genitori per la stesura finale dell'ePolicy
- Azione 2 Organizzare iniziative/incontri per consultare gli studenti sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- Azione 3 Organizzare eventi di presentazione del progetto Generazioni Connesse rivolto agli studenti/docenti e genitori

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

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

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

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

Il Liceo è da tempo attento allo sviluppo delle competenze digitali: per esempio nella progettazione di istituto, attraverso la programmazione dipartimentale e quella collegiale, sono presenti numerosi percorsi organizzati intorno ai seguenti Obiettivi formativi e competenze attese:

-Promuovere un uso consapevole, critico e creativo delle tecnologie, favorendo la conoscenza e l'uso dei linguaggi della comunicazione;

- Promuovere e sviluppare forme di apprendimento cooperativo, valorizzando le attività di gruppo come occasione di scambio e negoziazione di attitudini, conoscenze e capacità diverse;

- Approfondire le tematiche relative al rapporto adolescenti e nuove tecnologie;

- Far acquisire agli studenti strumenti specifici sui temi del bullismo e del cyberbullismo (privacy sul web, cyberbullismo, sexting; implicazioni giuridiche e psicologiche, funzionamento del web).

Con la DDI il digitale viene normato e normalizzato; la Legge 92/2019 che introduce l'insegnamento trasversale dell'Educazione Civica, dedica un intero articolo, il 5, alla Cittadinanza Digitale.

Il nostro Liceo, recependo il dettato normativo, ha elaborato un curricolo d'Istituto nel quale trova spazio e sistemazione l'educazione e lo sviluppo delle competenze digitali non solo come conoscenza tecnica degli strumenti ma soprattutto come uso consapevole critico e responsabile delle tecnologie digitali. Per le tematiche, i contenuti generali e il Profilo delle competenze per classi parallele si rimanda direttamente al curricolo di Educazione Civica di Istituto.

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

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

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

Il piano di formazione dei docenti sull' utilizzo delle TIC nella didattica, già avviato negli anni scorsi, prevede una parte dedicata all'alfabetizzazione digitale e una parte alla formazione metodologica.

Alfabetizzazione digitale: attività formative mirate allo sviluppo delle competenze digitali relative alle aree Informazione, comunicazione e creazione di contenuti del Digcomp 2.1(vedi **Piano di Formazione Docenti e PNSD nel PTOF**)

Formazione metodologica: attività formative e ricerca -azione dei

docenti sulle metodologie didattiche innovative mirate al superamento della didattica trasmissiva. (vedi adesione al **Movimento delle Avanguardie educative, Generazioni connesse e la piattaforma eTwinning)**.

Ai docenti sarà offerta la possibiltà di usufruire di attività formative organizzate dalla scuola e tenute da personale interno con adeguate competenze **(es. Animatore Digitale e Membri del Team per l'Innovazione),** o di partecipare alle proposte formative offerte da altre scuole, anche in rete come Future Smart Teacher. E' prevista anche la possibilità di autoaggiornamento fermo restando che tutte le attività di formazione devono essere in linea con le indicazioni contenute nel **Piano di Formazione dei Docenti** inserito nel PTOF.

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.

I docenti della scuola sono coinvolti in attività formative ed informative utili per la promozione e la condivisione di buone pratiche finalizzate all'uso consapevole delle TIC e la conoscenza dei rischi connessi al loro utilizzo.

Rispetto all'utilizzo non consapevole delle TIC sarà necessario individuare i risvolti emotivi e psicologici riguardo ai propri studenti. A motivo di ciò il Liceo prevede progetti specifici (inclusi nel PTOF); momenti di formazione specifica con la presenza di esperti; percorsi di formazione e/o autoaggiornamento come quello a cui la scuola ha partecipato sulla piattaforma di "Generazioni connesse" ; momenti seminariali ed eventi come il SID che la scuola organizza anche in accordo con scuole presenti sul territorio e la collaborazione delle Forze di Polizia .

Infine sul sito web della scuola è incluso un Google site "Cybersecurity" gestito dal referente del CB, in cui tutti gli utenti della comunità scolastica possono attingere per

la consultazione di materiali informativi,formativi e legislativi.

Gli utenti potranno altresì consultare il link del progetto di "Generazione connesse" e conoscere strumenti didattici utili per la prevenzione dei rischi legati a internet.

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

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

La scuola , consapevole dell'importanza del coinvolgimento dei genitori nella educazione digitale dei propri figli, sensibilizza le famiglie attraverso la documentazione informativa, i Regolamenti scolastici ,il Patto di corresponsabilità, e l' ePolicy al fine di far comprendere i principi che devono regolare l'utilizzo corretto delle TIC. A tal proposito la scuola

- presenta ai genitori il regolamento dell'ePolicy e li informa della presenza sul sito della scuola di una sezione dedicata;
- promuove la partecipazione degli stessi alla discussione e revisione del presente documento;
- favorisce incontri di consulenza con esperti;

- li coinvolge in iniziative in cui gli studenti sono protagonisti

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023)

- 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.
- 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.

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

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo 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.

La nostra scuola :

- garantisce la tutela in generale della privacy degli studenti ;

- definisce un regolamento per la gestione della privacy legata all'uso dei dispositivi ;

- adotta sistemi di sicurezza per la navigazione online sottolineando che dell' uso accidentale e improprio ai siti illeciti non può ritenersi responsabile.

- individua e definisce le misure di tutela, le modalità per garantirne nel tempo la continuità e l'adeguatezza e le responsabilità per la gestione dei dati: titolare, responsabile, persone autorizzate al trattamento.
- Il Liceo rispetta la privacy dei propri utenti e si impegna a proteggere i dati personali che gli stessi conferiscono all'istituzione, a trattarli in conformità alla normativa vigente.
- In caso di raccolta di dati personali, l'istituzione informerà l'utente sulle finalità della raccolta al momento della stessa, ove necessario, richiederà il consenso dell'utente.

L'Istituto non comunicherà i dati personali dell'utente a terzi senza il consenso dello stesso. Se l'utente decide di fornire alla scuola i propri dati personali, la scuola potrà comunicarli all'interno dell'Istituto od a terzi che prestano servizi alla scuola, solo rispetto a coloro che hanno bisogno di conoscerli in ragione delle proprie mansioni, e, ove necessario, con il permesso dell'utente.

La scuola tratta i dati personali dell'utente

- per soddisfare le richieste a specifici prodotti o servizi, per personalizzare la visita dell'utente al sito

- per aggiornare l'utente sulle ultime novità in relazione ai servizi offerti

- per comprendere meglio i bisogni dell'utente ed offrire allo stesso servizi migliori

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

- I video e le fotografie raccolte dai genitori durante le pubbliche attività scolastiche ,non violano la privacy

Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale e non alla diffusione.
Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime su Internet, e sui social network in particolare. (da vademecum privacy del Garante)
In caso di diffusione diventa necessario, di regola, ottenere il consenso informato delle persone presenti nelle fotografie e nei video.
Si deve quindi prestare attenzione prima di caricare immagini e video sui social network, oppure di diffonderle attraverso sistemi di messaggistica istantanea.

Tale pratica può dar luogo a gravi violazioni del diritto alla riservatezza delle persone riprese, e fare incorrere in sanzioni disciplinari, pecuniarie e in eventuali reati. (da vademecum privacy del Garante)

L'utilizzo di telefoni cellulari, di apparecchi per la registrazione di suoni e immagini, quando autorizzato dai docenti, è consentito, ma esclusivamente per fini personali, e sempre nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte (siano essi studenti o professori) in particolare della loro immagine e dignità.
La scuola ha, comunque, la possibilità di regolare o di inibire l'utilizzo di dispositivi elettronici all'interno delle aule o laboratori. Gli studenti e gli altri membri della comunità scolastica, in ogni caso, non possono diffondere o comunicare sistematicamente i dati di altre persone (ad esempio pubblicandoli su Internet) senza averle prima informate adeguatamente e averne ottenuto l'esplicito consenso. (da vademecum privacy del Garante).

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.

Il nostro Istituto ha provveduto a garatire la security per l'accesso a internet configurando dei filtri controllati dai gestori telefonici e dei firewall, per monitorare il traffico web e bloccare l'accesso a siti inappropriati; ha valutato tutti i rischi connessi alla sicurezza permettendo al personale scolastico l'accesso alla rete tramite i dispositivi della scuola o tramite i dispositivi personali nel caso del BYOD.

Ha aggiornato l'infrastruttura di rete, permettendo l'accesso a internet a tutte le classi.

Ha provveduto a gestire gli account di tutti gli utenti (studenti, insegnanti e personale ATA), ed attiverà il filtraggio dei contenuti e gli aspetti legali in relazione alla privacy.

Attraverso azioni del PNSD, la scuola è stata raggiunta da banda larga , sufficientemente veloce, per favorire l'uso di cloud per la didattica e l'uso di contenuti di apprendimento multimediali, attraverso cablaggio LAN e wireless in ogni spazio della scuola. Per l'accesso a internet

Gli studenti si impegnano a:

- utilizzare la rete nel modo corretto
- rispettare le consegne dei docenti
- non scaricare materiali e software senza autorizzazione

- non utilizzare unità removibili personali senza autorizzazione
- tenere spento lo smartphone al di fuori delle attività didattiche che ne prevedano l'utilizzo
- durante le attività che prevedono lo smartphone, utilizzarlo esclusivamente per svolgere le attività didattiche previste
- segnalare immediatamente materiali inadeguati ai propri insegnanti.

I docenti si impegnano a:

- utilizzare la rete nel modo corretto
- non utilizzare device personali se non per uso didattico
- formare gli studenti all'uso della rete
- dare consegne chiare e definire gli obiettivi delle attività

La scuola chiederà il consenso genitoriale a tutti i minorenni per l'uso di internet e per la pubblicazione di lavori e delle loro fotografie.Gli studenti con età superiore ai 16 anni (o maggiorenni) non hanno bisogno del consenso scritto dei genitori.

.

3.3 - Strumenti di comunicazione online

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

registro elettronico

Le famiglie ricevono le credenziali per l'accesso riservato al registro elettronico Argo ScuolaNext , in cui il corpo docente è tenuto a registrare

- assenze, valutazioni, note e osservazioni.

- risultati scolastici (voti, documenti di valutazione);

- prenotazioni colloqui individuali;

- eventi ;

- comunicazione varie .

La pubblicazione delle informazioni attraverso tale strumento assolve l'obbligo di comunicare prontamente ed efficacemente ogni evento riguardante gli alunni

e_mail

I docenti e il personale amministrativo possono utilizzare i servizi mail accedendo alla rete della scuola a fini esclusivamente didattici.
Gli stessi dispongono di un account G Suite_ Google Education con estensione @liceobertovibo.gov.it
L'account è strettamente personale, per cui ogni utente dovrà avere cura di disconnettere il proprio accesso al termine del suo utilizzo. Lo spazio del proprio account è destinato alla ricezione di comunicazioni, all'invio di documentazione e alla condivisione di materiali , progetti didattici o progetti con altri docenti. Sono attivi gli account per gli studenti, e create piattaforme di lavoro condiviso con Google Classroom per attività di e_learning.

La scadenza degli accessi sarà programmata al 31 agosto dell'anno di fine percorso scolastico. Lo stesso sarà per gli account dei docenti e del personale della scuola

Le comunicazioni tra personale scolastico, famiglie e studenti via e-mail avvengono tramite un indirizzo e-mail della scuola o tramite il registro elettronico Scuolanext DOCENTI_Scuolanext FAMIGLIA .
E-mail in arrivo ed allegati provenienti da mittenti sconosciuti non devono essere aperti.

sito della scuola

Il DS e il personale incaricato (in possesso di credenziali) hanno il compito di gestire il sito della scuola (www.liceobertovv.edu.it) e la responsabilità di garantire che i contenuti pubblicati e i servizi siano accurati e appropriati .

social network

I social network utilizzati per pubblicare commenti su persone e/o istituzioni ; diffondere foto/filmati senza il consenso degli utenti della comunità , possono causare reati penali.
Si invitano pertanto tutti gli studenti a non prelevare o diffondere immagini, video o registrazioni – anche solo audio – non autorizzate, ed eliminare da internet eventuali riferimenti offensivi o comunque illeciti (ed inopportuni) nei confronti dell'Istituto e dei suoi docenti e studenti.
Allo stesso tempo, si invitano gli allievi e i genitori a fare un uso prudente di Facebook e WhatsApp limitarndone l'uso alle sole comunicazioni funzionali.
.

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.

L'uso dei dispositivi personali in classe è normato dai seguenti regolamenti DPR n. 249/1998; DM n 30 del 15/03/2007 ; Regolamenti d'Istituto. In questi ultimi sono indicate le sanzioni disciplinari in caso di uso scorretto dei cellulari da parte dei ragazzi e delle ragazze in classe.

LINK AI REGOLAMENTI

Gli studenti

Per alunni in situazione di handicap, con DSA e BES, previa consultazione con il Consiglio di Classe, si concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili .

Se dovessero verificarsi eventi riconducibili all'uso non corretto o non legittimo di uno qualsiasi dei dispositivi , le reposnsabilità sono tutte ascrivibili alle famiglie degli studenti eventualmente coinvolti e condivise dal personale scolastico solo quando ,avendo personalmente constatato che qualche ragazzo/a fa uso di un device (smartphone o tablet) durante l'orario scolastico e lo utilizza in modo scorretto e contro il regolamento di istituto non dovesse immediatamente intervenire nelle forme già

indicate e comunque in modo tale da prevenire o reprimere sul nascere situazioni incompatibili con le più elementari regole della civile convivenza.

Il personale scolastico Docenti/ATA

Ai docenti è consentito utilizzare i dispositivi della scuola per realizzare tutte le attività connesse alla loro funzione.

E' consentito per i docenti l'uso dei propri dispositivi in classe per quanto attiene l'attività didattica qualora siano necessari, ma non possono essere utilizzati durante le lezioni per questioni personali.
Utilizzeranno la strumentazione fornita dalla scuola rispetto a quella personale , l' utilizzo improprio verrà contestato al titolare delle credenziali con cui è avvenuta la connessione.

Durante l'attività didattica il docente spiega ai propri alunni la netiquette e ne chiarisce le regole ; si assume la responsabilità di segnalare prontamente eventuali malfunzionamenti o danneggiamenti al tecnico informatico.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023).

- 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 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 il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti

- 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 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.*

Le azioni di sensibilizzazione e prevenzione rappresentano l'aspetto proattivo della scuola . Esse sono finalizzate a promuovere nei giovani le competenze e le capacità necessarie per una protezione adeguata , l'utilizzo consapevole delle TIC nonchè la gestione delle implicazioni. La scuola ha il compito di far comprendere agli studenti che il cambiamento può avvenire e deve essere soprattutto desiderato.

Tra le azioni che la scuola potrà prevedere

- coinvolgimento di tutte le componenti della comunità scolastica nella prevenzione e nel contrasto del bullismo e del cyberbullismo, favorendo la collaborazione dei genitori;
- attività laboratoriali specifiche sui temi da svolgere in classe ;
- integrazione della presente policy con il Regolamento di Istituto;
- comunicazione agli studenti e alle loro famiglie sulle sanzioni previste dal Regolamenti di Istituto nei casi di bullismo, cyberbullismo e navigazione online a rischio;
- monitoraggio e informazione alla comunità scolastica della situazione reale della scuola ; valutazione oggettiva dell'efficacia degli interventi attuati;
- eventi formativi rivolti ai docenti, genitori sulle problematiche del bullismo e del cyberbullismo impostati anche sulla base dell'analisi dei bisogni;
- consulenza presso servizi deputati ad offrire un supporto psicologico e/o di mediazione
- ricorso a procedure codificate per segnalare alle famiglie e/o organismi competenti i comportamenti a rischio;

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

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

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

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

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

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

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

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

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

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

relazione a questa problematica.

Da implementare con le indicazioni contenute nella lezione.

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?

Da implementare con le indicazioni contenute nella lezione.

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.

Da implementare con le indicazioni contenute nella lezione.

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.

Da implementare con le indicazioni contenute nella lezione.

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.

Da implementare con le indicazioni contenute nella lezione.

Il nostro piano d'azioni

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

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

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

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

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

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

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

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

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

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

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

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

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

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.

Come si evince dagli obiettivi prioritari (ART. 1, COMMA 7 L. 107/15) elencati nel PTOF, i Regolamenti d'Istituto , l'Atto d'indirizzo e il Patto di corresponsabilità, il Liceo è aperto alla collaborazione con le famiglie e gli enti locali coinvolti per la formazione di un ambiente sereno e accogliente in cui tutte le forze in campo interagiscano per contrastare atti di bullismo e/o cyberbullismo e promuovere una partecipazione attiva e responsabile di tutte le componenti della comunità scolastica.

Il Lliceo si preoccuperà di condurre un'opera di sensibilizzazione rivolta alle famiglie e agli studenti riguardo ai possibili rischi della navigazione online (Cyberbullismo, Adescamento online, Sexting,Dipendenza da Internet, videogiochi, shopping o gambling online, ... Esposizione a contenuti pornografici, violenti, razzisti, Violazione della privacy.)e le opportunità offerte dalla scuola per far fronte ad eventuali problemi. Oltre agli incontri con esperti già precedentemente indicati, sarà arricchita la sezione dedicata al Cyberbullismo presente sul sito della scuola con video, guide in pdf, manuali e links a siti istituzionali, come quello della Polizia postale, o specializzati come il sito di Generazioni connesse.

Studenti, genitori, insegnanti e tutto il personale della scuola avrà modo di segnalare eventuali comportamenti a rischio per poter attuare le modalità d'intervento più idonee.

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.

Nel caso A in cui si abbia il sospetto di un possibile abuso riferibile a uno dei casi elencati prima, si seguirà la seguente procedura:

- il personale docente o il personale scolastico, si rivolge al referente per il Cyberbullisomo che verificherà la situazione e informerà il Dirigente Scolatico.
- lo studente o gli studenti possono rivolgersi al Coordinatore di Classe, o ad un docente della classe o direttamente al referente Cuyberbullismo per segnalare l'abuso;
- i genitori si possono rivolgere al Coordinatore di Classe o al Referente Cyberbullismo o al Dirigente Scolastico.

Nel caso B :

- il docente o il personale scolastico informa il referente Cyberbullismo e il Dirigente Scolastico in maniera da intervenire tempestivamente e impedire ulteriori problemi.
-
- lo studente o gli studenti possono rivolgersi al Coordinatore di Classe, o ad un docente della classe o direttamente al referente Cuyberbullismo per segnalare l'abuso;

- i genitori si possono rivolgere al Coordinatore di Classe o al Referente Cyberbullismo o al Dirigente Scolastico.
- Il Dirigente Scolastico, valutata la gravità dell'episodio insieme al Referente Cyberbullismo, si rivolge agli organi competenti in materia.

5.3. - Gli attori sul territorio

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

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

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

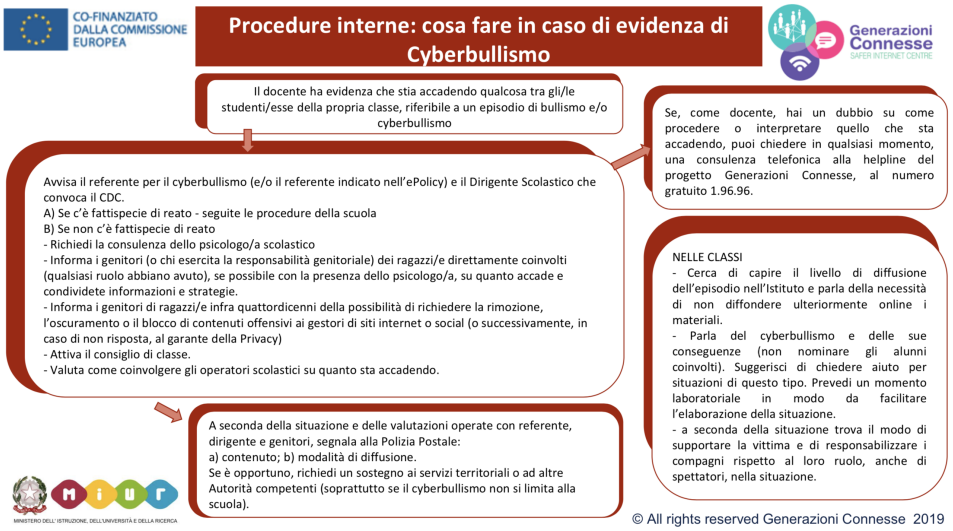
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni**: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico**:

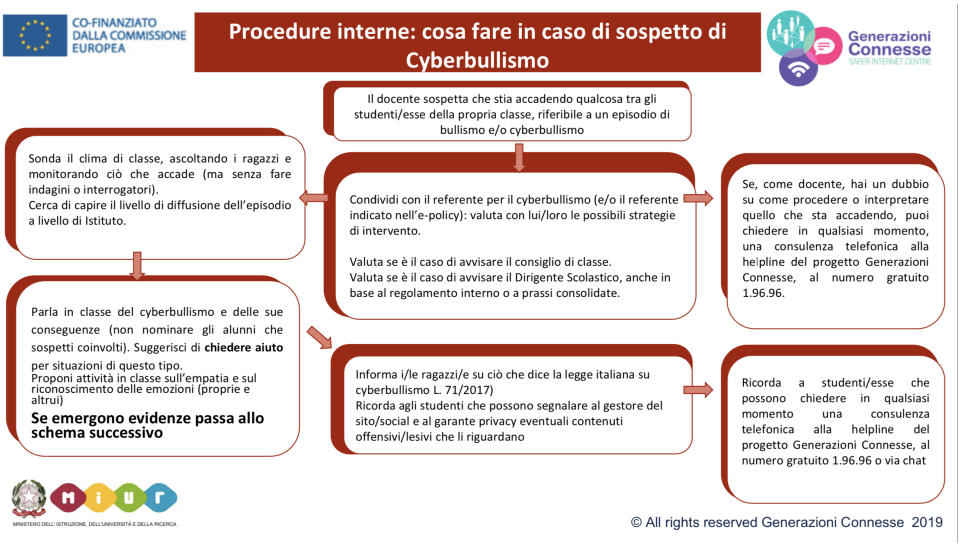
segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.

- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

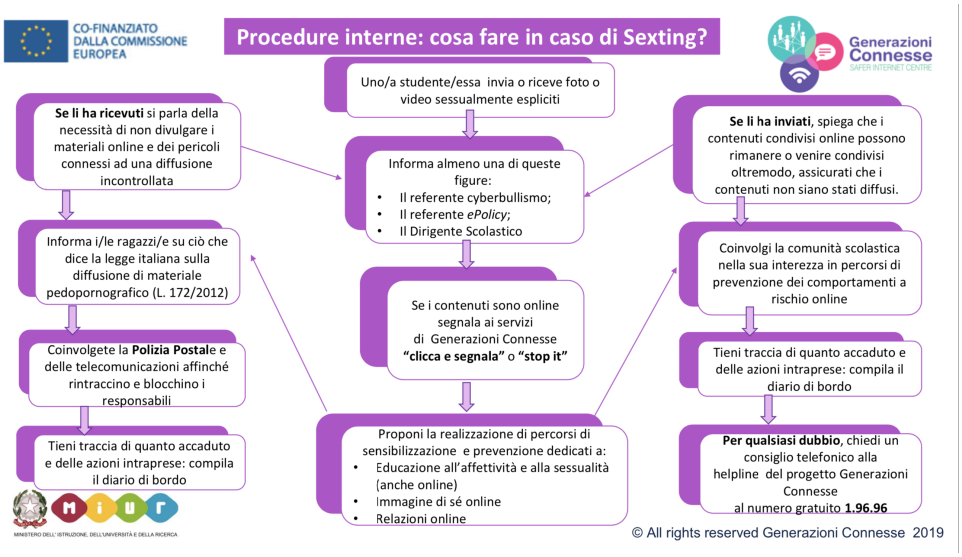
5.4. - Allegati con le procedure

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

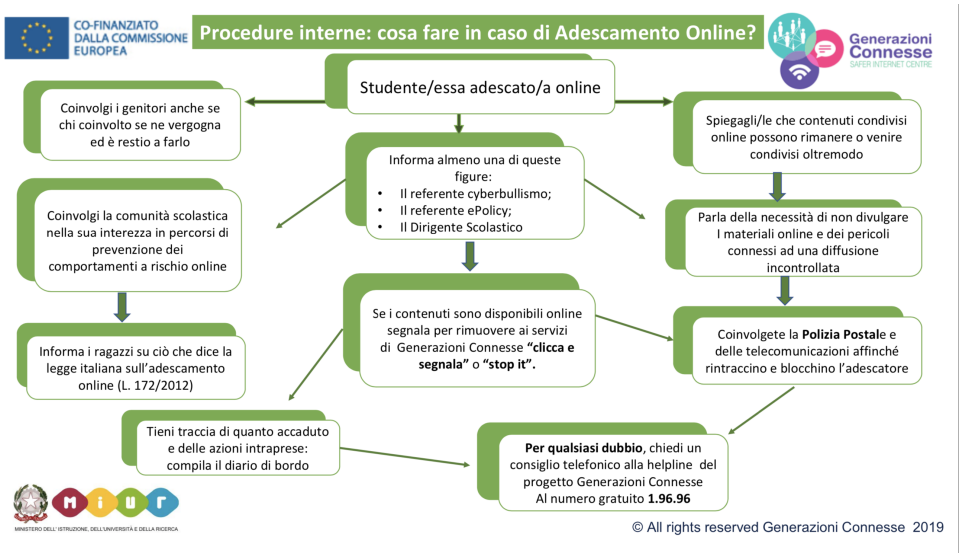




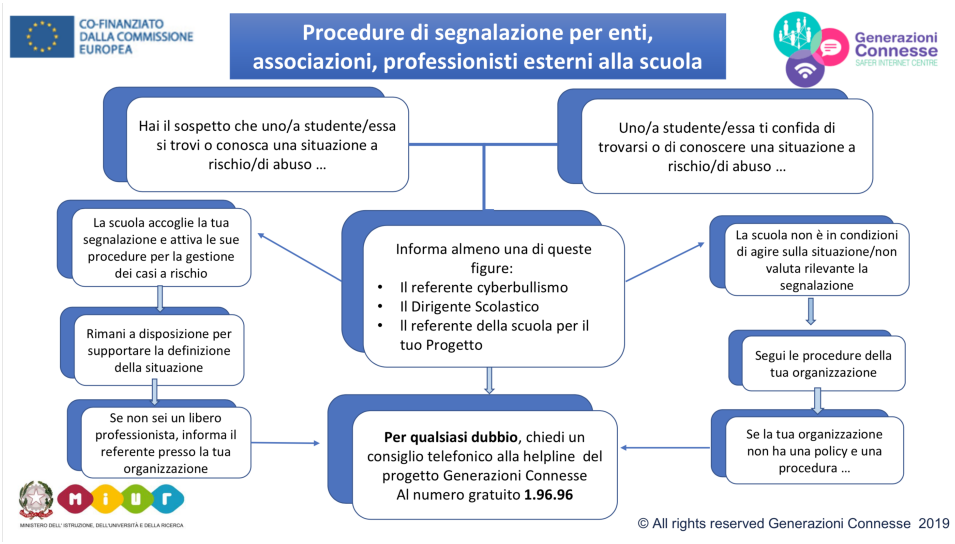
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

In appendice oltre agli Allegati forniti dalla piattaforma "Generazioni connesse" per la rilevazione e la gestione dei casi , seguomo

- Liberatoria _LICEO SCIENTIFICO G. BERTO

- modello segnalazione casi

- modello monitoraggio dei casi segnalati_diario di bordo

- modello segnalazione Garante per la protezione dei dati personali

Il nostro piano d'azioni

Non è prevista nessuna azione.

Generazioni Connesse
SAFER INTERNET CENTRE

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

Co-financed by the European Union
Connecting Europe Facility

LICEO SCIENTIFICO G. BERTO

MODULO PER LA SEGNALAZIONE DI CASI

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

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

MODULO PER IL FOLLOW-UP DEI CASI

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

LICEO SCIENTIFICO G. BERTO VV

Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi

Scuola _____ Anno Scolastico _____

N°	Data	ora	Episodio *(riassunto)*	Azioni intraprese		Insegnante con cui l'alunno/a si è confidato	Firma
				Cosa?	Da chi?		

Modello per segnalare episodi di bullismo sul web o sui social network e chiedere l'intervento del Garante per la protezione dei dati personali

Con questo modello si può richiedere al Garante per la protezione dei dati personali di disporre **il blocco/divieto della diffusione online di contenuti ritenuti atti di cyberbullismo** ai sensi dell'art. 2, comma 2, della legge 71/2017 e degli artt. 143 e 144 del Codice in materia di protezione dei dati personali, d. lg. n. 196 del 2003, come modificato dal decreto legislativo 10 agosto 2018, n. 101

INVIARE A

Garante per la protezione dei dati personali
indirizzo e-mail: cyberbullismo@gpdp.it

IMPORTANTE - La segnalazione può essere presentata direttamente da chi ha un'età maggiore di 14 anni o da chi esercita la responsabilità genitoriale su un minore.

CHI EFFETTUA LA SEGNALAZIONE?

(Scegliere una delle due opzioni e compilare TUTTI i campi)

☐ Mi ritengo vittima di cyberbullismo e sono un minore che ha compiuto 14 anni	Nome e cognome Luogo e data di nascita Residente a Via/piazza Telefono E-mail/PEC
☐ Sono un adulto che ha responsabilità genitoriale su un minore di 14 anni che si ritiene vittima di cyberbullismo	Nome e cognome Luogo e data di nascita Residente a Via/piazza Telefono E-mail/PEC **Chi è il minore vittima di cyberbullismo?** Nome e cognome Luogo e data di nascita Residente a Via/piazza

IN COSA CONSISTE L'AZIONE DI CYBERBULLISMO DI CUI TI RITIENI VITTIMA?

(indicare una o più opzioni nella lista che segue)

- ☐ pressioni
- ☐ aggressione
- ☐ molestia
- ☐ ricatto
- ☐ ingiuria
- ☐ denigrazione
- ☐ diffamazione
- ☐ furto d'identità *(es: qualcuno finge di essere me sui social network, hanno rubato le mie password e utilizzato il mio account sui social network, ecc.)*
- ☐ alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali *(es: qualcuno ha ottenuto e diffuso immagini, video o informazioni che mi riguardano senza che io volessi, ecc.)*
- ☐ qualcuno ha diffuso online dati e informazioni (video, foto, post, ecc.) per attaccare o ridicolizzare me, e/o la mia famiglia e/o il mio gruppo di amici

QUALI SONO I CONTENUTI CHE VORRESTI FAR RIMUOVERE O OSCURARE SUL WEB O SU UN SOCIAL NETWORK? PERCHE' LI CONSIDERI ATTI DI CYBERBULISMO?

(Inserire una sintetica descrizione – **IMPORTANTE SPIEGARE DI COSA SI TRATTA**)

_____

_____

_____

_____

_____

DOVE SONO STATI DIFFUSI I CONTENUTI OFFENSIVI?

- ☐ sul sito internet [è *necessario indicare l'indirizzo del sito o meglio l'URL specifico*]
  _____
- ☐ *su uno o più social network* [*specificare su quale/i social network e su quale/i profilo/i o pagina/e in particolare*] _____
- ☐ altro [*specificare*] _____

Se possibile, allegare all'e-mail immagini, video, *screenshot* e/o altri elementi informativi utili relativi all'atto di cyberbullismo e specificare qui sotto di cosa si tratta.

1) _____

2) _____

3) _____

HAI SEGNALATO AL TITOLARE DEL TRATTAMENTO O AL GESTORE DEL SITO WEB O DEL SOCIAL NETWORK CHE TI RITIENI VITTIMA DI CYBERBULLISMO RICHIEDENDO LA RIMOZIONE O L'OSCURAMENTO DEI CONTENUTI MOLESTI?

☐ Si, ma il titolare/gestore non ha provveduto entro i tempi previsti dalla Legge 71/2017 sul cyberbulllismo *[allego copia della richiesta inviata e altri documenti utili]*;

☐ No, perché non ho saputo/potuto identificare chi fosse il titolare/gestore

HAI PRESENTATO DENUNCIA/QUERELA PER I FATTI CHE HAI DESCRITTO?

☐ Si, presso _____;

☐ No

Luogo, data

Nome e cognome

Si ricorda che chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice in materia di protezione dei dati personali (Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante), salvo che il fatto non costituisca più grave reato.

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Il Garante per la protezione dei dati personali (con sede in Piazza Venezia n. 11, IT-00187, Roma; Email: protocollo@gpdp.it; PEC: protocollo@pec.gpdp.it; Centralino: +39 06696771), in qualità di titolare del trattamento, tratterà i dati personali conferiti con il presente modulo con modalità prevalentemente informatiche e telematiche, per le finalità previste dal Regolamento (Ue) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196 e s.m.i.), in particolare per lo svolgimento dei compiti istituzionali nell'ambito del contrasto del fenomeno del cyberbullismo.

Il conferimento dei dati è obbligatorio e la loro mancata indicazione non consente di effettuare l'esame della segnalazione. I dati acquisiti nell'ambito della procedura di esame della segnalazione saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa.

I dati saranno trattati esclusivamente dal personale e da collaboratori dell'Autorità o delle imprese espressamente nominate come responsabili del trattamento. Al di fuori di queste ipotesi, i dati non saranno diffusi, né saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli ad altri soggetti coinvolti nell'attività istruttoria e nei casi specificamente previsti dal diritto nazionale o dell'Unione europea.

Gli interessati hanno il diritto di ottenere dal Garante, nei casi previsti, l'accesso ai propri dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (art. 15 e ss. del Regolamento). L'apposita istanza all'Autorità è presentata contattando il Responsabile della protezione dei dati presso il Garante (Garante per la protezione dei personali - Responsabile della Protezione dei dati personali, Piazza Venezia, 11, 00187, Roma, email: rpd@gpdp.it).