LICEO delle SCIENZE UMANE

TORNIELLI BELLINI

Documento di ePolicy

NOPM010005

LICEO DELLE SCIENZE UMANE C.T. BELLINI"

BALUARDO LAMARMORA 10 - 28100 - NOVARA - NOVARA (NO)

Maria Motta

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.

1.1 SCOPO DELL'E-POLICY

La presenza sempre più capillare delle nuove tecnologie nella vita quotidiana di ognuno ha

inevitabilmente interessato la scuola nelle sue multiformi realtà.

In quest'anno scolastico 2019-2020, per la pandemia COVID19, tutti i docenti hanno messo in atto strategie di didattica a distanza per poter rispondere ai bisogni educativi e formativi degli studenti.

L'uso della tecnologia ha supportato l'apprendimento ed ha permesso agli studenti di sperimentare un nuovo approccio alla didattica e allo studio, una diversa relazione tra pari e con i docenti. Si è creata una relazione basata sulla responsabilità e la centralità del proprio ruolo in cui ogni discente è diventato parte attiva e responsabile del percorso d'apprendimento.

Da oggi sicuramente molte cose cambieranno e la tecnologia giocherà un ruolo sempre più importante all'interno del curriculo formativo degli studenti. In quest'ottica, occorre accompagnare gli studenti nella acquisizione di un uso corretto delle nuove tecnologie, attraverso lo sviluppo della "competenza digitale", fondamentale nella vita di oggi e nei percorsi formativi o lavorativi futuri.

L'E-policy è un documento programmatico prodotto dall'Istituzione Scolastica volto a descrivere:

- il proprio approccio alle tematiche legate alle competenze digitali, alla sicurezza online e ad un uso positivo delle tecnologie digitali nella didattica,
- le norme comportamentali e le procedure per l'utilizzo delle Tecnologie dell'informazione e della comunicazione (ICT) in ambiente scolastico, le misure per la prevenzione riguardo alla cybersecurity e rispetto delle norme su privacy, copyright
- le misure per la rilevazione e gestione delle problematiche connesse ad un uso non corretto delle tecnologie digitali.

1.2 - Ruoli e responsabilità

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

1.2 RUOLI E RESPONSABILITA'

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 promuove:

- una formazione interna adeguata del personale scolastico

- un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line
- il supporto ai docenti nelle procedure per la segnalazione e gestione dei casi che dovessero verificarsi per garantire la sicurezza, anche online, di tutti i membri della comunità scolastica.
- la cultura della sicurezza online
- l'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull' utilizzo positivo e responsabile delle TIC

Il Dirigente Scolastico ha la responsabilità:

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

L'Animatore Digitale

L'Animatore digitale, gli Assistenti Tecnici e il team per il P.N.S.D si occupano, cooperando, di:

- favorire la formazione interna per lo sviluppo della "scuola digitale" e per la sicurezza in rete
- individuare i fabbisogni ICT dell'istituto
- cogliere e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di Internet a scuola,
- proporre soluzioni metodologiche didattiche innovative e tecnologiche sostenibili (progetti, azioni didattico-educative, organizzazione incontri e conferenze in sede, partecipazione ad eventi aziendali con le classi)
- supportare il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali
- monitorare e rilevare eventuali episodi o problematiche connesse all'uso delle TIC a scuola
- controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione)

In particolare l'Animatore digitale ha il compito di:

- supportare il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali
- promuovere percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio, allo sviluppo delle competenze digitali previste anche nell'ambito dell'educazione civica)
- monitorare e rilevare eventuali episodi o problematiche connesse all'uso delle TIC a scuola
- controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

- individuare i fabbisogni ICT dell'istituto
- cogliere e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di Internet a scuola,
- proporre soluzioni metodologiche didattiche innovative e tecnologiche sostenibili (progetti, azioni didattico-educative, organizzazione incontri e conferenze in sede, partecipazione ad eventi aziendali con le classi)
- promuovere la salvaguardia dei dati e da attacchi alla sicurezza della rete (aggiornamenti frequenti firewall, software di rete, antivirus, backup dati)

Animatore digitale e gli Assistenti Tecnici per il P.N.S.D si occupano anche di Misure di prevenzione dei rischi on line

1) Prevenzione riguardo alle minacce agli strumenti ICT:

- tenere aggiornato il sistema operativo dei dispositivi fissi e mobili connessi in rete
- installare e tenere aggiornato frequentemente il programma antivirus e browser
- attivare la funzione firewall del S.O. (da pannello di controllo) connesso al server di rete
- tenere il livello di sicurezza a media - alto nelle impostazioni del browser per la navigazione nella rete internet

2) Prevenzione riguardo agli accessi ad Internet:

- tenere riservate le credenziali (LOGIN e PASSWORD) di accesso alla rete Internet
- tenere riservate le credenziali di accesso a servizi Internet
- scegliere una password di almeno otto caratteri alfanumerici
- non accedere ai siti web non certificati e nascosti (DEEP WEB)
- non aprire email con mittente sconosciuto e non scaricare allegati
- non fornire proprie credenziali richieste tramite email (PHISHING)
- tenersi aggiornati su i siti web:

http://www.miur.gov.it/-/il-6-febbraio-e-il-safer-internet-day

http://www.generazioniconnesse.it/site/it/home-page

3) Prevenzione riguardo normative privacy e copyright:

- formazione educativa sul rispetto della privacy delle persone (legge 196/2003)
- non fare foto e video senza autorizzazione delle persone ritratte o riprese, e se minorenni senza autorizzazione di entrambi i genitori
- non pubblicare dati personali completi (cognome, nome, data e luogo di nascita propri ed altrui su social media, forum e siti web non conosciuti)
- non utilizzare prodotti intellettuali digitali (foto, video, e-book, etc) senza rispettare il

copyright o creative commons nel web che non concedono il loro uso.
- non utilizzare dispositivi e non fare foto o videoregistrazioni se non autorizzati ai fini didattici dal docente durante l'attività didattica.

Il Referente bullismo e cyberbullismo che "Ogni Istituto scolastico, nell'ambito della propria autonomia, individua fra i docenti [...] con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo" (Art. 4 Legge n.71/2017) ha il compito di:

- coordinare e promuovere iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio.)
- coinvolgere, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori

I Docenti rivestono un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete ed hanno il compito di:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di Internet rispettando e facendo rispettare il regolamento di Istituto
- garantire che le modalità di utilizzo corretto delle TIC e di Internet siano inerenti le attività didattiche ed educative delle classi;
- garantire che gli alunni comprendano le opportunità offerte dalle modalità digitali e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di INTERNET
- 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: Registro elettronico, sito web scolastico in cui i fornitori di questi servizi informatici sono garanti del trattamento dei dati personali GDPR e della sicurezza
- assicurare la riservatezza dei dati personali e sensibili trattati ai sensi della normativa vigente anche nelle comunicazioni digitali ;
- controllare il buon utilizzo delle tecnologie nei laboratori, nelle aule LIM, dei dispositivi mobili, macchine fotografiche, smart watch etc.. da parte degli alunni durante le attività scolastiche (ove consentito dal docente)
- guidare gli alunni nell'utilizzo siti web certificati e verificati come adeguati per il loro uso nelle ricerche e produzioni tramite la rete Internet
- comunicare con i genitori in caso di difficoltà, bisogni (BES/PDP) espressi dagli alunni, utilizzo non rispettoso del regolamento tramite annotazioni disciplinari (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC e di Internet
- segnalare qualsiasi problema o proposta (progetto) ovvero esigenza di carattere didattico/formativo all'animatore digitale ai fini della ricerca di soluzioni metodologiche didattiche e tecnologiche innovative e di un aggiornamento delle TIC nei laboratori e nelle

aule

- segnalare al dirigente scolastico ed alla referente Cyberbullismo 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 e della comunicazione ai genitori.
- dare chiare indicazioni sul corretto utilizzo della rete scolastica, indicando agli alunni le regole di istituto
- segnalare eventuali malfunzionamenti o danneggiamenti ai tecnici informatici
- non divulgare le proprie credenziali di accesso degli account Lan e della rete Wi-Fi d'istituto
- non allontanarsi dalla postazione lasciandola incustodita, se non prima di aver effettuato la disconnessione dal proprio account in particolare per chiudere il registro elettronico
- non salvare sul disco locale della postazione in istituto file contenenti dati personali e sensibili
- ripulire la propria cartella sul server della Lan scolastica da file non più utili, fare copia dei propri file importanti in cloud o usb key
- integrare parti del curriculum della propria disciplina con approfondimenti ad hoc, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica
- accompagnare e supportare gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete
- hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse.

Il personale Amministrativo, Tecnico e Ausiliario (ATA) svolge funzioni miste, ossia di tipo amministrativo, contabile, gestionale e di sorveglianza connesse all'attività delle istituzioni scolastiche, in collaborazione con il dirigente scolastico e con il personale docente tutto. Diverse figure che, in sinergia, si occupano ciascuno per la propria funzione, del funzionamento dell'Istituto scolastico che passa anche attraverso lo sviluppo della cultura digitale e dell'organizzazione del tempo scuola. Esiste, cioè, un concreto coinvolgimento del personale ATA nell'applicazione della legge 107/15 ("La Buona Scuola") che concerne non solo il tempo scuola e il potenziamento dell'offerta formativa, ma anche le attività di formazione e autoformazione in tema di bullismo e cyberbullismo.

Il personale ATA che deve essere coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo / cyberbullismo ha il compito di:

- raccogliere, verificare e valutare le informazioni inerenti possibili casi di bullismo /

cyberbullismo.

Gli Studenti e le Studentesse

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

- rispettare il regolamento di istituto in generale ed in particolare sul corretto utilizzo delle TIC, della rete e dei dati propri ed altrui.
- collaborare con i docenti per una cittadinanza digitale comprendendo le potenzialità offerte dalle TIC e dalla rete Internet
- conoscere e rispettare la privacy, il diritto d'autore, le buone pratiche di sicurezza web.
- adottare condotte rispettose degli altri anche quando si comunica in rete.
- comunicare con gli adulti di riferimento sull'uso e sui rischi delle tecnologie e della rete.
- utilizzare le TIC su indicazioni del docente;
- accedere all'ambiente di lavoro con il corretto account, non divulgandone le credenziali di accesso ed archiviare i propri documenti in maniera ordinata e facilmente rintracciabile nella cartella personale presente nel Server;
- in caso di riscontro di malfunzionamenti della strumentazione e/o di contatto accidentale con informazioni, immagini e/o applicazioni inappropriate comunicarlo immediatamente all'insegnante;
- non eseguire tentativi di modifica della configurazione di sistema delle macchine;
- non utilizzare la strumentazione della scuola a scopi personali, ludici e/o ricreativi;
- non utilizzare propri dispositivi esterni personali senza aver acquisito il permesso da parte dell'insegnante;
- chiudere correttamente la propria sessione di lavoro
- utilizzare al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti; con il supporto della scuola
- imparare a tutelarsi online, tutelare i/le propri/e compagni/e e rispettarli/le
- partecipare attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete
- farsi promotori di quanto appreso anche attraverso possibili percorsi di peer education;

I Genitori, in continuità con l'Istituto scolastico, hanno il dovere di:

- collaborare con la comunità scolastica educativa per l'utilizzo consapevole delle TIC e rispettoso delle normative vigenti in materia;
- proporre buone pratiche educative per un utilizzo corretto delle TIC e della rete
- monitorare ed attivare un controllo parentale verso siti web non certificati (giochi, scommesse, deep web), social media con pubblicazione foto e video che possano compromettere il benessere dei propri figli o dei loro compagni od amici

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

Gli Enti educativi esterni e le associazioni che entrano in relazione con la scuola hanno il compito di:

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

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

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

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

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

1.3 UN'INFORMATIVA PER I SOGGETTI ESTERNI CHE EROGANO ATTIVITÀ EDUCATIVE NELL'ISTITUTO

Quanti entrano in contatto con gli studenti e le studentesse sono tenuti a mantenere in ogni

circostanza un comportamento professionale, serio, moralmente ineccepibile ma anche franco ed aperto, naturalmente disposto all'ascolto dei bisogni dei ragazzi: è evidente che a scuola 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. A tutti coloro che hanno accesso ai locali dell'Istituto è fatto obbligo di conoscere e rispettare le regole adottate per l'impiego dei dispositivi personali e/o in dotazione della scuola, a maggior ragione quando entrano in contatto con gli allievi. La privacy di tutti i soggetti (minorenni e non) è tutelata in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

In Allegato si trova l'informativa per i soggetti esterni.

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.

1.4 CONDIVISIONE E COMUNICAZIONE DELL'E-POLICY ALL'INTERA COMUNITÀ SCOLASTICA

Il presente documento, frutto di un lavoro di condivisione e confronto con la partecipazione di docenti e famiglie, è reso oggetto di condivisione da parte dell'intera comunità scolastica sia in fase di elaborazione (attraverso il coinvolgimento delle famiglie), sia attraverso l'approvazione da parte degli Organi Collegiali.

Di esso viene data ampia diffusione a tutta la Comunità Scolastica, attraverso la pubblicazione sul sito web istituzionale

---

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.

1.5 GESTIONE DELL'INFRAZIONE ALLA E-POLICY

Il Referente per il bullismo e il suo team sono coloro ai quali bisogna rivolgersi immediatamente nel caso in cui si verifichino comportamenti dubbi o nascano sospetti di violazioni. Questi in giornata riferiranno al Dirigente che avrà cura di convocare le parti interessate onde valutare le possibili azioni da intraprendere.

.

Al personale, agli studenti e agli altri componenti della comunità scolastica sono date informazioni sulle infrazioni previste e le eventuali sanzioni graduate in modo proporzionale rispetto alla gravità dell'azione compiuta attraverso il Regolamento di Istituto. (art. 4 DPR 249 del 1998)

Le sanzioni riferite soprattutto agli alunni avranno come carattere preferenziale quello educativo/riabilitativo e in ogni caso verrà coinvolta la componente genitori, in qualità di primi educatori.

È fondamentale per l'Istituto, anche nella sanzione, creare sempre occasioni di recupero. Risulta infatti possibile commutare i giorni di sospensione con attività socialmente utili interne alla scuola o presso strutture opportunamente individuate dal Consiglio di Classe.

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.

1.6 INTEGRAZIONE DELL'E-POLICY CON REGOLAMENTI ESISTENTI

L'Istituto, che per vocazione e per curricolo da sempre mette in primo piano l'interesse per la persona e i suoi bisogni educativi, sociali e formativi, ha già inserito nel Patto di corresponsabilità attività orientate alla prevenzione di ogni forma di prevaricazione. Il ruolo delle famiglie e degli studenti è attivo e centrale: sono chiamati infatti a collaborare con la scuola perché tutte le iniziative messe in campo possano sviluppare la coscienza sociale e formare il cittadino di domani.

Il Patto di corresponsabilità è un documento che si modifica e si arricchisce ogni volta che si offrono alla scuola opportunità nuove di crescita.

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.

1.7 MONITORAGGIO DELL'IMPLEMENTAZIONE DELLA E-POLICY E SUO AGGIORNAMENTO

La e-safety policy sarà riesaminata annualmente e/o quando si verificheranno cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola. In questo processo verrà coinvolto tutto il personale docente.

Sarà rivista in relazione a norme di maggior valore come regolamenti o Policy emanati dal MIUR o eventuali leggi dello Stato.

Al fine di monitorare tale documento la scuola organizzerà, dove possibile anche attraverso video-conferenze on line:

10. 1 evento di presentazione del progetto Generazioni Connesse rivolto agli studenti

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Organizzare uno o più eventi o attività (anche online) volti a presentare il progetto a studenti, docenti e genitori e consultare i docenti dell'Istituto per la stesura finale dell'ePolicy.

Azioni da svolgere nei prossimi 3 anni:

- Organizzare uno o più eventi o attività (anche online) volti a presentare il progetto ai nuovi studenti, docenti, genitori.
- Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell'ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.

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.

2.1 Curricolo sulle competenze digitali per gli studenti

La competenza digitale è la quarta delle competenze chiave per l'apprendimento permanente e, nella Raccomandazione del Parlamento Europeo e del Consiglio del 18 dicembre 2006, viene descritta come "[...] il saper utilizzare, con dimestichezza e spirito critico, le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata dalle abilità di base nelle TIC (Tecnologie di Informazione e di Comunicazione): l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet.".

DESTINATARI: biennio LSU e LES

DURATA: i due anni scolastici del biennio

TRIENNIO: lo sviluppo delle skills digitali all'interno della formazione finalizzata ai PCTO.

OBIETTIVI E TEMI DA AFFRONTARE

Il curriculo delle competenze digitali richiama diverse aree: la dimensione tecnologica, quella cognitiva e la sicurezza.

Il curricolo è strutturato in 5 aree di competenza (C) descritte in termini di evidenze osservabili (performance, abilità, capacità) indicate con A. In corrispondenza di ciascuna evidenza, è riportato un breve elenco di attività o contenuti che possono attivare le relative evidenze. Tale elenco è fornito senza pretesa di esaustività, come spunto operativo per strutturare in modo coerente le attività disciplinari con la didattica digitale.

C1 – Informazione: identificare, localizzare, recuperare, conservare, organizzare e analizzare le informazioni digitali, giudicando la loro rilevanza e finalità.

A1 – Esplorare, cercare e selezionare le informazioni: accedere e cercare informazioni on line, articolare i bisogni informativi, trovare le informazioni rilevanti, selezionare le risorse in maniera efficace, navigare tra le risorse on line, sviluppare strategie personali per trovare informazioni.

[utilizzo interfaccia di un web browser, personalizzare le funzioni di un browser, criteri di ricerca in un motore di ricerca, creare un alert, iscriversi ad una newsletter, condividere informazioni utilizzando pulsanti di sharing, portali per l'informazione, portali con risorse educative, servizi di traduzione, …]

A2 – Valutare le informazioni: raccogliere, elaborare, comprendere e valutare criticamente le

informazioni.

[impostazioni di ricerca avanzata in un motore di ricerca, copiare/incollare/tagliare o effettuare screenshot di informazioni rilevanti ed organizzarle in un software di videoscrittura, utilizzare software per mappe concettuali, utilizzare software per modificare file pdf facilitandone lettura e ricerca di informazioni …]

A3 – Conservare e recuperare le informazioni: manipolare e conservare le informazioni e i contenuti per essere poi recuperati, organizzare le informazioni e i dati.

[utilizzare servizi computing di cloud, creazione di cartelle e gruppi di file su PC o dispositivo mobile, organizzare i file con i tag, memorie di massa, …]

C2 – Comunicazione: comunicare nel contesto digitale, condividere risorse attraverso strumenti on line, collegarsi con gli altri e collaborare attraverso strumenti digitali, interagire nelle comunità partecipando con consapevolezza interculturale.

A1 – Interagire per mezzo di tecnologie: interagire attraverso una varietà di strumenti e

applicazioni, comprendere come la comunicazione digitale è distribuita, presentata e gestita, comprendere la vie appropriate per comunicare attraverso i mezzi digitali, far riferimento ai differenti formati di comunicazione, adattare i modi e le strategie del comunicare alle differenti audience. [messaggistica istantanea, posta elettronica, videochiamate, integrazione tra software per la comunicazione, social networking,…]

A2 – Condividere informazioni e contenuti: condividere con gli altri le locazioni e i contenuti delle informazioni trovate, condividere la conoscenza, i contenuti e le risorse, agire come un intermediario, essere proattivo nel diffondere notizie, contenuti e risorse, conoscere le pratiche di citazione e integrare le nuove informazioni nell'insieme delle conoscenze esistenti. [piattaforme web 2.0 per la condivisione e la diffusione delle informazioni (Youtube, Dailymotion, Facebook, Twitter, … e integrazione tra sistemi, sistemi di costruzione collaborativa del sapere (Wikipedia, Citizendium, Debatepedia …]

A3 – Collaborare attraverso canali digitali: usare le tecnologie e i media per lavorare in team, per processi collaborativi, e per la co-costruzione e co-creazione di risorse, conoscenza e contenuti.

[software di scrittura collaborativa (Collabedit, Google Documents, Mimio, IWB su Android Survio, Socrative), partecipare ad un gruppo di discussione (G+, Facebook, …)]

A4 – Netiquette: avere la conoscenza e il sapere pratico delle norme di comportamento nelle interazioni on line e virtuali, essere consapevole dei diversi aspetti culturali, essere abile nel proteggere se stesso e gli altri da possibili pericoli on line (es. cyber bullying), sviluppare strategie attive per scoprire comportamenti inappropriati.

A5 – Gestire l'identità digitale: creare, adattare e gestire una o molteplici identità digitali, essere capace di proteggere la propria reputazione; gestire sia dati che prodotti attraverso

molteplici accounts e applicazioni. [gestione di account]

C3 Creazione di contenuti: creare ed editare nuovi contenuti (da testi elaborati digitalmente a immagini e video), integrare e rielaborare conoscenze precedenti e contenuti, produrre espressioni creative, prodotti multimediali e programmi, tener conto e applicare le questioni di proprietà intellettuale e le licenze.

A1 – Sviluppare contenuti: creare contenuti di diverso formato, inclusi i multimediali, editare e migliorare contenuti creati da sé o dagli altri, esprimersi creativamente attraverso i media digitali e le tecnologie.

[software di presentazione (PowerPoint, Padlet, Presentazioni google, …), software di videoscrittura, software di calcolo…

A2 – Integrare e rielaborare: modificare, rifinire e integrare risorse esistenti per sviluppare nuovi, originali e rilevanti contenuti e conoscenze.

[software e app per la modifica creativa di immagini e testi, editing di materiale video, editing di materiale audio, creazione di e-book …]

A3 – Copyright e licenze: comprendere come si applicano al caso dell'informazione e del contenuto copyright e licenze.

A4 – Programmazione: utilizzare installazioni, modifiche dei programmi, utilizzo dei programmi.

[principi fondamentali (terminologia, navigazione, funzionalità) dei dispositivi digitali, digitalizzazione, utilizzo del computer, ingresso in un nuovo programma, ...]

C4 Sicurezza: protezione personale, protezione dei dati, protezione dell'identità digitale, misure di sicurezza, usi sicuri e sostenibili.

A1 – Proteggere gli strumenti: proteggere i propri strumenti e capire i rischi e le minacce on line, conoscere le misure da adottare per la sicurezza.

A2 – Proteggere i dati personali: comprensione dei termini comuni di un sevizio; attiva protezione dei dati personali; comprensione dell'altrui privacy; proteggere se stessi dalle frodi on line, dalle minacce e dal bullismo informatico (cyber).

A3 – Proteggere la salute: evitare i rischi per la salute nell'uso della tecnologia in termini di minacce al benessere fisico e psicologico.

C5 Problem solving: identificare bisogni e risorse digitali, prendere decisioni informate su quali siano i più adatti strumenti digitali sulla base delle finalità e dei bisogni, risolvere questioni concettuali mediante strumenti digitali, uso creativo delle tecnologie, risolvere problemi tecnici, aggiornare le proprie e altrui competenze.

A1 – Risolvere problemi tecnici: identificare possibili problemi e risolverli (da piccole disfunzioni a problemi più complessi) con l'aiuto di mezzi digitali.

[conoscenza del sistema operativo, operazioni di base di configurazione di un computer o dispositivo mobile, gestione delle reti ...]

A2 – Identificare bisogni e risposte tecnologiche: valutare i propri bisogni in termini di sviluppo di risorse, strumenti e competenze, collegare bisogni e possibili soluzioni, adattare strumenti ai bisogni personali, valutare criticamente possibili soluzioni e strumenti digitali.

A3 – Innovare e usare creativamente le tecnologia: realizzare innovazioni con le tecnologie, partecipare attivamente e collaborativamente nella produzione digitale e multimediale, esprimere creativamente se stessi attraverso i media e le tecnologie digitali, creare conoscenza e risolvere problemi concettuali con l'aiuto di strumenti digitali.

DOCENTI COINVOLTI: ANMATORE DIGITALE CON IL SUPPORTO DEGLI ASSISTENTI TECNICI NELLE FASI FORMATIVE E COME SUPPORTO e i docenti dell'Istituto.

I docenti che utilizzano le nuove tecnologie dovranno contribuire alla realizzazione del curriculo all'interno delle lezioni nell'attuazione di progetti multimediali volti ad un utilizzo consapevole, creativo e critico della tecnologia.

MONITORAGGIO DEL PERCORSO

Rubrica di valutazione / questionario

C1 Informazione

Livello base: Esegue qualche ricerca on line per mezzo di motori di ricerca. Salva e immagazzina file e contenuti (testi, immagini, musica, video, pagine web). Recupera ciò che ha salvato. È consapevole che non tutta l'informazione on line è affidabile.

Livello intermedio: Esplora internet per informazioni e cerca informazioni on line. Seleziona le informazioni che trova. Confronta le differenti fonti di informazione. Salva, immagazzina file, contenuti e informazioni e personalizza le strategie di conservazione. Recupera e gestisce le informazioni e i contenuti salvati e conservati.

Livello avanzato: È in grado di usare una grande varietà di strategie per cercare informazioni ed esplorare internet. È critico nei riguardi delle informazioni che trova e sa verificarne validità e credibilità. Filtra e monitora le informazioni che riceve. Usa differenti metodi e strumenti per organizzare file, contenuti e informazioni. Utilizza varie strategie per recuperare e gestire i contenuti ha organizzato e conservato. Seleziona in modo appropriato gli ambienti di condivisione delle informazioni (micro-blog).

C2 comunicazione

Livello base: Interagisce con gli altri utilizzando gli elementi essenziali degli strumenti di comunicazione (telefoni mobili, Voip, chat, e-mail). Conosce le fondamentali norme di comportamento nella comunicazione con strumenti digitali. Condivide con gli altri file e contenuti attraverso semplici mezzi tecnologici. Utilizza in modo passivo, sollecitato o marginale i servizi della rete. Comunica prevalentemente con le tecnologie tradizionali. È consapevole dei benefici e dei rischi relativi all'identità digitale.

Livello intermedio: È in grado di usare molteplici mezzi digitali, anche avanzati, per interagire con gli altri: conosce i principi dell'etichetta digitale ed è capace di utilizzarli nel proprio contesto.

Partecipa nei siti di reti sociali e nella comunità on line, dove comunica o scambia conoscenze, contenuti e informazioni.

Valorizza alcune delle principali caratteristiche dei servizi on line. Crea e discute risultati in collaborazione con altri usando semplici mezzi digitali.

Livello avanzato: È impegnato nell'uso di un ampio spettro di mezzi per la comunicazione on line (e-mail, chat, sms, instant messages, blog, micro-blog…). È in grado di applicare i vari aspetti dell'etichetta on line ai vari ambiti e contesti della comunicazione digitale. Ha sviluppato strategie per scoprire comportamenti inappropriati. Configura il formato e la via comunicativa in funzione della propria audience. Gestisce i differenti tipi di comunicazione che riceve. È in grado di scambiare attivamente informazioni, contenuti e risorse con gli altri attraverso comunità on line, reti

e piattaforme comunicative. Partecipa attivamente ad ambienti on line. Si impegna attivamente nella partecipazione on line e utilizza molteplici servizi online. Utilizza in modo efficace e funzionale mezzi e vie di collaborazione per la produzione e condivisione di risorse, conoscenze e contenuti. È in grado di gestire molteplici identità digitali a seconda dei contesti e delle finalità, e può monitorare informazioni e dati prodotti attraverso l'interazione on line.

C3 Creazione di contenuti

Livello base: Produce semplici contenuti digitali (testi, tabelle, immagini, audio,…). Modifica in maniera essenziale quanto prodotto da altri. Modifica qualche semplice funzione dei software utilizzati. È consapevole che alcuni contenuti trovati sono coperti da copyright.

Livello intermedio: Produce contenuti digitali di differente formato (testi, tabelle, immagini, video…). Modifica e rifinisce i contenuti prodotti da sé o da altri. Possiede le conoscenze fondamentali riguardo le differenze tra copyright, furto di copyright e creative commons e sa

attribuire un valore di licenza ai contenuti che crea. Esegue varie forme di modifica del software e delle applicazioni (installazione avanzate, modifiche di programma essenziali…).

Livello avanzato: Produce contenuti digitali in differenti formati, piattaforme a ambienti. Utilizza una varietà di mezzi digitali per creare prodotti multimediali originali. È in grado di integrare elementi di contenuto esistenti per crearne di nuovi. Sa come i differenti tipi di licenze si applicano alle informazioni e risorse che utilizza o crea. Interagisce con programmi (aperti) modificandoli secondo le proprie preferenze.

C4 - sicurezza

Livello base: Prende le fondamentali misure per proteggere i propri strumenti (antivirus, password). È consapevole che deve condividere solo alcune tipologie di informazioni su se stesso e gli altri in ambienti on line. Sa come evitare tentativi di cyber bullying. Sa che la tecnologia può influenzare la propria salute, se utilizzata in modo inappropriato. Prende le misure di base per risparmiare energia.

Livello intermedio: Protegge i propri strumenti digitali, aggiornando le strategie di sicurezza. Proteggere la propria riservatezza in modo adeguato. Comprende i problemi di privacy e ha una conoscenza base di come i suoi dati sono raccolti e usati. Protegge se stesso e gli altri da cyber bullying. Comprende i rischi per la salute collegati all'uso delle tecnologie (da problemi di ergonomia a dipendenza).

Livello avanzato: Aggiorna frequentemente le proprie strategie di sicurezza. Conosce misure di sicurezza quando i propri strumenti sono minacciati. Cambia spesso le forme di garanzia della privacy. Ha una comprensione informata e ampia dei problemi della privacy e sa come i propri dati sono raccolti e usati. È consapevole di come usare le tecnologie per evitare problemi di salute. È equilibrato nel gestire la relazione tra mondo online e mondo offline. Ha una posizione informata sull'impatto delle tecnologie sulla vita quotidiana, sui consumi online e sull'ambiente.

C5 problem solving

Livello base: Ricorre in modo mirato ad aiuti e assistenze quando le tecnologie non funzionano o utilizza nuovi strumenti, programmi o applicazioni. Usa alcune tecnologie per risolvere compiti di routine. Sceglie strumenti digitali per attività di routine. Sa che le tecnologie e gli strumenti digitali possono essere usati creativamente e riesce in un numero relativamente limitato di volte.

Livello intermedio: Risolve semplici problemi che emergono quando le tecnologie non funzionano. Sceglie l'hardware e il software appropriato per un'azione. Risolve compiti non di routine esplorando le possibilità tecnologiche. Seleziona un appropriato mezzo in base alle finalità e ne valuta l'efficacia. Utilizza le tecnologie per fini creativi e le finalizza alla risoluzione dei problemi. Collabora con gli altri nella creazione di prodotti innovativi.

Livello avanzato: Risolve un ampio spettro di problemi emergenti nell'uso di tecnologie. Prende decisioni informate per scegliere mezzi, strumenti, applicazioni, software o servizi per compiti non familiari. È consapevole dei nuovi sviluppi tecnologici. Comprende come i nuovi strumenti lavorano e operano. Valuta criticamente quale è il miglior strumento per una determinata azione. Risolve questioni concettuali con il supporto di strumenti tecnologici e digitali.

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.

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

Le TIC devono essere utilizzate ad integrazione della didattica al fine di progettare, sviluppare, utilizzare, gestire e valutare i processi d'insegnamento e apprendimento di tutti gli studenti e le studentesse della classe, anche delle persone con disabilità (in chiave inclusiva).

Verranno pianificati in tal senso corsi formativi per i docenti attraverso docenti formati, dall'animatore digitale e dal supporto delle reti di scuole e dall'amministrazione, sia quelle scelte liberamente dai docenti (anche on line), purché restino coerenti col piano di formazione.

FINALITA': utilizzare le TIC in maniera strutturata e integrata per rendere gli apprendimenti più motivanti, coinvolgenti ed inclusivi per guidare gli studenti verso una fruizione di contenuti on line. Si sviluppano capacità quali il lavoro di gruppo, anche a distanza. Competenza utile nel mondo lavorativo.

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.

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

Corsi tenuti da esperti esterni (polizia postale, nucleo di prossimità, scuole Polo USR, osservatori generali sul bullismo ecc..) sull'uso responsabile e sicuro della rete ma anche i rischi legati a quest'ultime. La formazione permette di dare ai docenti gli strumenti per educare i ragazzi e le ragazze alle emozioni in contesto onlife e quindi modulare e gestire i propri ed altrui comportamenti, favorendo e promuovendo forme di convivenza civile.

a. s. 2019-2020 corsi on line sulla DAD

a. s. 2020-2021 analisi dei bisogni formativi dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica, alla luce dell'esperienza dell'anno precedente.

Organizzare incontri formativi in presenza, a scuola con esperti esterni, enti o associazioni.

Monitoraggio delle azioni attraverso questionari valutativi.

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.

2.4 - Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

a.s.2019-2020 due percorsi proposti ai genitori dal nucleo di prossimità locale sul Rischio del Web e dei giochi on line.

a.s. 2020-2021 possibile aggiornamento del patto di corresponsabilità con le famiglie e predisposizione di percorsi per i genitori sulle tematiche relative alle TIC, con il coinvolgimento del nucleo di prossimità e degli studenti formati nell'anno scolastico 2019-2020 dal Gruppo Noi della scuola.

Il nostro piano d'azioni

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

Scegliere almeno 1 di queste azioni

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

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

Scegliere almeno 1 di queste azioni

- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

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.

3.1 Protezione delle strumentazioni e della navigazione

La scuola, attraverso una policy sviluppata nel corso degli anni, adotta tutte le strategie per:

a) Proteggere la privacy del personale scolastico, degli alunni e delle loro famiglie, soprattutto per quel che riguarda i dati sensibili.

b) Garantire la navigazione sicura nei computer dell'Istituto attraverso:

5. Antivirus (software per il monitoraggio e la rimozione di virus, spyware, adware)
6. Filtri (sistemi in grado di bloccare in modo automatico l'utilizzo di determinati servizi o l'accesso a siti e contenuti potenzialmente dannosi per adolescenti)
7. Utenti diversificati (Utente docente, utente alunno, utente genitore e utente personale scolastico protetto da password per l'accesso al registro Elettronico e alle piattaforme didattiche)

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.

3.2 Gestione accessi

a) Accesso alle strumentazioni scolastiche

Il personale scolastico è tenuto a seguire le seguenti regole di accesso alle strumentazioni:

5. È consentito l'uso delle strumentazioni scolastiche esclusivamente per uso didattico. Usi diversi da questo vanno autorizzati dal Dirigente Scolastico.
6. Le strumentazioni scolastiche devono essere maneggiate con attenzione al fine di evitarne danni strutturali.
7. Il personale scolastico è tenuto a segnalare tempestivamente al responsabile della custodia delle strumentazioni la mancanza delle stesse o di eventuali accessori.
8. Le strumentazioni vanno custodite in appositi armadi provvisti di serratura. Laddove ciò non fosse possibile.
9. L'utente riservato ai docenti è essere provvisto di password (che non deve essere comunicata in nessun casi agli alunni).
10. Non è consentito il salvataggio di documenti personali (bollette telefoniche, cedolini stipendi, ecc).
11. È vietato installare software nelle strumentazioni, l'installazione spetta gli assistenti tecnici previa autorizzazione da parte del Dirigente.

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

5. È consentito l'uso delle strumentazioni scolastiche esclusivamente per uso didattico, secondo le disposizioni del docente presente.
6. Le strumentazioni scolastiche devono essere maneggiate con attenzione al fine di evitarne danni strutturali.
7. Gli alunni possono accedere solo all'utente a loro riservato, corrispondente alla classe.
8. È consentito il salvataggio di documenti personali a scopo didattico, utilizzando cartelle specifiche per ciascuna classe.

b) Accesso alla rete

Nella nostra scuola esistono due reti LAN interne che si collegano entrambe alla fibra ottica: una rete è dedicata alla didattica (aule, laboratori, biblioteca) una all'amministrazione (segreteria, presidenza e vicepresidenza, aula magna, auditorium, aula 30 pc docenti). Per motivi di sicurezza le due reti sono separate ed accedono a due server diversi. L'accesso alla rete è permesso solo attraverso autenticazione personale (rete amministrativa) e/o autentificazione di classe (rete didattica). L'accesso alla wireless avviene attraverso autenticazione che viene fornita ai soli docenti. Tutte le aule e i device possono collegarsi alla rete wireless, la gestione delle autenticazione è affidata agli assistenti tecnici.

c) Accesso ad internet

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

5. È possibile accedere ad internet attraverso strumentazioni in dotazione all'istituto o attraverso dispositivi personali.
6. L'accesso ad internet e la navigazione attraverso le strumentazioni scolastiche è riservato ad un uso strettamente didattico.
7. È possibile accedere ad account personali durante l'uso di internet, ma è obbligatorio il logout al termine.
8. Non è consentito il salvataggio di dati personali (nomi utenti, account e password) nei browser delle strumentazioni scolastiche.
9. È vietato scaricare o installare da internet materiale potenzialmente dannoso, di provenienza non sicura o non legale.

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

5. L'accesso ad internet e la navigazione attraverso le strumentazioni scolastiche è riservato ad un uso strettamente didattico e nel rispetto di diritti della cittadinanza digitale e delle norme vigenti di utilizzo legale della rete.
6. È vietato il salvataggio di dati personali (nomi utenti, account e password) nei browser delle strumentazioni scolastiche.
7. È vietato scaricare da internet materiale senza l'autorizzazione del docente.

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

previste per il personale.

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.

3.3 E-mail

Tutte le comunicazioni scolastiche dovranno progressivamente avvenire attraverso canali digitali. Il personale scolastico, le famiglie, gli operatori esterni e gli Enti potranno comunicare con la segreteria inviando la posta all'indirizzo istituzionale NOPM01005@istruzione.it o agli indirizzi indicati nella sezione contatti del sito. I docenti possiedono, su richiesta, un indirizzo di posta istituzionale. L'uso personale e non scolastico delle web mail è vietato e sanzionato con l'interdizione dall'uso delle stesse.

3.4 Blog

Un blog è un particolare tipo di sito web che può essere assimilato a un diario personale o a un giornale: uno o più autori scelgono un tema e lo argomentano o pubblicano il resoconto di fatti accaduti. Attualmente la nostra scuola non possiede un Blog. Qualora l'Istituto decidesse di aprire un blog, il TID avrà cura di aggiornare il presente documento con un regolamento d'utilizzo.

3.5 Sito web della scuola

Il sito scolastico è stato ristrutturato completamente nel 2018 ed ha i seguenti parametri:

Dominio: www.liceobellini.edu.it Il sito scolastico viene tempestivamente aggiornato secondo le norme vigenti sulla trasparenza e in particolare:

5. La pubblicazione delle informazioni e delle circolari nella Homepage, nell'Albo on line e nell'Amministrazione Trasparente è a cura del personale di segreteria.

6. Le altre sezioni e la struttura stessa del sito vengono aggiornate dall'Animatore Digitale secondo necessità.
7. L'accesso alla sezione amministrativa del sito scolastico è riservata al Dirigente Scolastico, al personale di segreteria e all'Animatore Digitale, con utenze diversificate.
8. L'accesso alla parte pubblica del sito è libera.
9. Alcune informazioni possono essere tenute riservate in sezioni protette del sito, accessibili agli utenti dell'Istituto tramite registrazione (personale interno e docenti).

3.6 Social network

È vietato al personale scolastico e agli alunni di accedere a social network e chat attraverso le strumentazioni della scuola, se non per uso didattico. In caso di progetti che ne prevedano l'uso, il docente è tenuto a monitorare gli alunni affinché ne facciano un uso corretto, secondo le disposizioni dell'insegnante. È comunque vietato pubblicare sui social network o su qualunque sito internet documenti, foto, registrazioni audio-video che possano essere lesivi per la reputazione o per la privacy degli alunni e del personale scolastico. Segnalazioni di infrazioni possono essere comunicate secondo il protocollo presente al capitolo 5.

3.7 Registro

Il registro elettronico on line è uno strumento al quale possono accedere tutti i membri della Comunità Scolastica, previa registrazione da parte degli assistenti tecnici. Tutti gli utenti devono essere provvisti di nome utente e password. L'uso del registro è personale e riservato: ogni utente deve provvedere affinché i dati di login restino riservati e si impegna a cambiare password nel caso in cui la riservatezza degli stessi sia stata violata. Il sistema cambia in ogni caso la password ogni 180 giorni.

a) Area Amministrativa

Il Dirigente scolastico, il personale di segreteria, gli Assistenti tecnici e l'Animatore digitale possono accedere a specifiche aree riservate, personalizzate secondo ruoli e mansioni stabilite, per configurare le impostazioni di sistema e inviare comunicazioni al personale.

b) Area Docenti

Il personale scolastico può accedere solo all'area riservata ai docenti. I dati di accesso all'account devono essere richiesti personalmente agli Assistenti tecnici del registro o in segreteria. Il personale scolastico:

5. È tenuto a leggere le comunicazioni del sistema su eventuali aggiornamenti.
6. Può inviare comunicazioni e avvisi ai genitori tramite l'apposita sezione.
7. Può pubblicare e condividere con docenti e alunni materiale didattico.
8. Deve registrare quotidianamente le presenze e firmare il registro di classe.
9. Deve tenere periodicamente aggiornate le sezioni riguardanti le assenze e i voti.
10. Deve compilare le proposte di voto e indicare le assenze entro i termini previsti per lo scrutinio.
11. Deve comunicare alla segreteria eventuali incongruenze nell'elenco degli alunni.
12. Deve segnalare all'Animatore digitale del registro eventuali anomalie nel funzionamento.

c) Area Tutori

I genitori (tutori) accedono all'apposita sezione ad essi riservata ed hanno a disposizione due account diversificati (uno per genitore). I dati di accesso all'account vengono consegnati personalmente ai genitori delle classi prime. I genitori, non presenti in tale occasione o i genitori di alunni trasferiti in corso d'anno, devono richiedere i dati di accesso in segreteria e ritirarli personalmente. I genitori:

5. Sono tenuti a leggere le comunicazioni ufficiali della segreteria sul sito web e dei docenti sul registro elettronico.
6. Devono controllare quotidianamente il registro, in particolare le assenze, i voti, le note.
7. Possono effettuare le prenotazioni dei colloqui con i docenti.
8. Possono rispondere alle comunicazioni del personale docente solo attraverso la mail istituzionale NOPM010005@istruzione.it.
9. Devono comunicare alla segreteria eventuali incongruenze nei dati anagrafici personali o del proprio figlio.
10. Devono segnalare ai docenti eventuali anomalie nel funzionamento o incongruenze nei dati inseriti.
11. Devono mantenere riservati i dati di accesso.

d) Area alunni

Gli alunni accedono all'apposita sezione ad essi riservata ed hanno a disposizione un account dedicato. I dati di accesso all'account vengono consegnati personalmente agli alunni delle classi prime. Gli alunni trasferiti in corso d'anno, devono richiedere i dati di accesso in segreteria e ritirarli personalmente. Gli alunni:

5. Sono tenuti a leggere le comunicazioni ufficiali della segreteria sul sito web e dei docenti sul registro elettronico.

6. Devono controllare quotidianamente il registro, in particolare le assenze, i voti, le note, gli argomenti delle lezioni, i compiti assegnati e i documenti condivisi.
7. Possono effettuare le prenotazioni dei colloqui con i docenti per i propri genitori.
8. Devono comunicare alla segreteria eventuali incongruenze nei dati anagrafici personali.
9. Devono segnalare ai docenti eventuali anomalie nel funzionamento o incongruenze nei dati inseriti.
10. Devono mantenere riservati i dati di accesso.

3.8 Protezione dei dati personali

Si ricorda a tutto il personale scolastico che il segreto professionale o d'ufficio obbliga a non rivelare le informazioni aventi natura di segreto, secondo un codice etico (legato al rispetto della persona), deontologico (come norma di comportamento professionale) e giuridico. È conseguentemente vietato al personale scolastico di divulgare personalmente o di pubblicare su blog, social network o siti personali qualunque informazione possa violare il segreto d'ufficio.

Procedure operative per la protezione dei dati personali.

3.4 - Strumentazione personale

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

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

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

Per quanto riguarda dati di accesso a strumentazioni, reti wi-fi o registri, tutti i dipendenti devono:

5. Custodire i dati di accesso facendo attenzione che terzi non ne vengano a conoscenza.
6. Nel caso in cui sia violata la segretezza di una password, il personale deve provvedere alla sua immediata sostituzione (nel caso di password personale) o alla repentina comunicazione al personale responsabile (nel caso di password condivise impostate dall'Amministratore della rete).

Il personale scolastico, nello svolgimento delle proprie mansioni, deve prestare particolare attenzione a:

5. Non divulgare ad estranei le informazioni di cui viene a conoscenza durante il servizio.
6. Non fare copie, per uso personale, dei dati sensibili.
7. Osservare i criteri di riservatezza.
8. Trattare i dati in modo lecito e secondo correttezza.
9. Trattare i dati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati.
10. Comportarsi nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione, di perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Il personale di segreteria e gli assistenti tecnici sono inoltre tenuti a:

5. Provvedere al salvataggio di backup periodici (almeno settimanali) su supporti esterni che dovranno essere opportunamente conservati e non accessibili a persone non autorizzate
6. Adottare delle cautele nella trasmissione, nella riproduzione e nella distruzione dei documenti contenenti dati personali, al fine di prevenire eventuali rischi di accesso ai dati da parte di soggetti non autorizzati.
7. Per tutte le procedure inerenti la sicurezza e la gestione dei dati fare riferimento ai documenti interni previsti dalle norme.

L'Amministratore di rete, l'Animatore digitale e l'Assistente tecnico, che possiedono dati di accesso a reti, siti, registri, strumentazioni per lo svolgimento delle specifiche mansioni, sono inoltre tenuti a:

5. Non comunicare a persone non autorizzate i dati di accesso di terzi in loro possesso
6. Non utilizzare i dati di accesso di terzi senza motivata ragione

Il nostro piano d'azioni

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

- 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 (già svolti i webinar su Cisco, RE in cui si sono affrontati anche temi riguardanti la sicurezza dei dati).

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

- Realizzazione di una piattaforma di condivisione e gestione delle video conferenze (Gsuite)
- Realizzazione di caselle di posta istituzionale per tutti i docenti dell'Istituto
- 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.*

4.1 SENSIBILIZZAZIONE E PREVENZIONE

L'evolversi del mondo virtuale e della tecnologia ha determinato, tra l'altro, la dematerializzazione dei rapporti interpersonali, realizzando comunicazioni a distanza tra gli individui ed identità indefinite, come quelle dei "falsi profili". La possibilità di agire in anonimato e l'assenza di concreti limiti spaziali, consentita dai dispositivi tecnologici, hanno generato una nuova e pericolosa modalità di espressione del bullismo: il bullismo cibernetico o cyberbullismo, che si esplica attraverso i comportamenti aggressivi o violenti, tipici del bullismo, ma realizzati con il tramite di

strumentazione informatica e telematica.

La scuola ha il dovere di far conoscere i rischi legati ad un utilizzo non consapevole del digitale e della Rete. Se, dunque, le Tecnologie dell'Informazione e della Comunicazione (TIC) sono parte integrante della vita quotidiana dei più giovani, in quanto strumenti privilegiati di comunicazione e di relazione, ma anche di informazione, studio, creatività e partecipazione, esse pongono però delle questioni associate alla "sicurezza" e al comportamento sociale. Non bisogna, infatti, cadere nello stereotipo di una categoria uniforme di bambini/e e adolescenti "competenti", sollevando gli adulti dal proprio ruolo educativo e dalla responsabilità di promuovere presso i più giovani un uso consapevole e quindi anche un uso integrativo (e non sostitutivo) delle tecnologie digitali. Siamo di fronte ad una realtà complessa, pensata prevalentemente per un mondo adulto e nella quale trovano spazio contenuti e comportamenti potenzialmente dannosi.

Per questo, in particolare, nel biennio i docenti, l'animatore digitale ed altri attori lavorano sulla costruzione delle competenze digitali o meglio delle competenze di cittadinanza digitale.

Quando si parla di rischio si fa riferimento alla possibilità per il minore di:

1. commettere azioni online che possano danneggiare se stesso o altri
2. essere una vittima di queste azioni
3. osservare altri commettere queste azioni

I rischi online rappresentano tutte quelle situazioni problematiche derivanti da un uso non consapevole e non responsabile delle tecnologie digitali da parte di bambini/e, ragazzi e ragazze: adescamento online, cyberbullismo, sexting, violazione della privacy, pornografia (recenti ricerche hanno sottolineato come la maggior parte degli adolescenti reperisca in Rete informazioni inerenti la sessualità, col rischio, spesso effettivo, del diffondersi di informazioni scorrette e/o l'avvalorarsi di falsi miti), pedopornografia (con questo termine si intende qualsiasi foto o video di natura sessuale che ritrae persone minorenni), gioco d'azzardo o gambling, internet addiction, videogiochi online (alcuni rischi associati possono essere ad esempio: contatti impropri con adulti, contenuti violenti e/o inadeguati; acquisti incontrollati, etc.), esposizione a contenuti dannosi o inadeguati (es. contenuti razzisti, che inneggiano al suicidio, che promuovono comportamenti alimentari scorretti, etc.), etc.

Partendo da questo punto di vista, vanno promosse nei più giovani le necessarie competenze e capacità, per una protezione adeguata, ma anche per un utilizzo consapevole che sappia sfruttare le potenzialità delle tecnologie digitali e gestirne le implicazioni.

Due sono i principali strumenti in questo caso da mettere in campo e si sintetizzano in interventi di Sensibilizzazione e Prevenzione.

AZIONI INTRAPRESE DALLA SCUOLA

La prima forma di prevenzione è quella Universale, diretta a tutta la comunità scolastica,

programmata e proposta da più soggetti che operano in sinergia a 360° su tutta la comunità scolastica. Le azioni sono:

1. interventi di esperti esterni alla scuola tenuti dal nucleo di prossimità e dalla polizia postale per gli studenti, i genitori e, dal prossimo anno, per tutto il personale scolastico e gli ATA.
2. percorsi di peer educator grazie al Progetto per Tommaso e alla costituzione del Gruppo Noi; in cui i ragazzi vengono educati ad educare, supportare e, nel caso sia necessario, segnalare casi legati a fenomeni di bullismo e cyberbullismo.
3. interventi dei peer formati nelle classi, attraverso tavole rotonde, per accrescere la consapevolezza nel gruppo target di riferimento circa un determinato tema/bisogno/problema che potrebbe presentarsi in quel gruppo nella scuola. Lo scopo è quello d'incoraggiare il gruppo a modificare i propri comportamenti rendendoli più funzionali e diffondere all'esterno del gruppo di riferimento e quindi tra l'opinione pubblica una certa consapevolezza rispetto all'argomento di interesse.
4. interventi dei peer del Progetto per Tommaso, con la supervisione dei referenti del progetto nelle scuole medie per sensibilizzare gli studenti su queste tematiche.
5. interventi del referente del cyberbullismo e del Team di riferimento, per favorire la diffusione di informazioni e servizi disponibili all'utilità collettiva (ad es., si può pensare ad un intervento di sensibilizzazione per promuovere la conoscenza dell'E-Policy nella comunità scolastica)
6. attivazione dello sportello "Generazioni Connesse", gestito da docenti specializzati, che offrono un servizio di ascolto e raccolgono le prime segnalazioni su queste tematiche; compilano il modulo di prima segnalazione e girano subito il medesimo alla referente del bullismo e cyberbullismo. A seconda della gravità, il referente con il team preposto (ed in casi molto gravi, la DS) attiverà due tipologie di percorsi, identificati in due livelli:

1. prevenzione Selettiva: un programma dedicato ad un gruppo di studenti in cui il rischio online è presente. In questo caso la presenza del rischio è stata individuata tramite indagini, segnalazioni, oppure dalla conoscenza della presenza di fattori di rischio in quel determinato territorio. In questi casi gli interventi sono mirati e prevedono programmi formativi strutturati (con i docenti, la psicologa della scuola, attraverso letture, lavori di gruppo) che hanno l'obiettivo di migliorare le competenze digitali e le strategie di problem solving. Può essere un valido programma se si osservano casi in cui la prevenzione universale non ha dato gli esiti previsti.
2. prevenzione Indicata: un programma di intervento sul caso specifico è quindi pensato e strutturato per adattarsi agli/lle studenti/studentesse con l'obiettivo di ridurre i comportamenti problematici, oppure dare supporto alle vittime. Per la sua natura questo tipo di intervento si avvale di professionalità diverse perché spesso affronta problemi legati alla salute mentale del minore per cui è opportuno coinvolgere anche la famiglia del/la ragazzo/a.

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).

4.2 CYBERBULLISMO CHE COS’È E COME PREVENIRLO

La definizione è contenuta nel comma I dell’art. 1 della Legge 71/2017 (legge Ferrara): “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”.

È possibile suddividere gli atti di cyberbullismo in due grandi gruppi:

- cyberbullismo diretto: il bullo utilizza strumenti di messaggistica istantanea (es. sms, mms) che hanno un effetto immediato sulla vittima, poiché diretti esclusivamente a lei.
- cyberbullismo indiretto: il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima anche da un punto di vista psicologico.

È molto importante sottolineare come il cyberbullismo non sia una problematica che riguarda unicamente vittima e cyberbullo. È un fenomeno sociale e di gruppo. Infatti, centrale è il ruolo delle agenzie educative e di socializzazione (formali e informali) più importanti per gli adolescenti: la famiglia, la scuola, i media, le tecnologie digitali e il gruppo dei pari.

Per prevenire tale fenomeno tutta la comunità scolastica deve assumersene la responsabilità attraverso la conoscenza del fenomeno, per riconoscerlo e quindi prevenirlo

Ecco alcuni segnali generali che la potenziale vittima di cyberbullismo può manifestare:

1. appare nervosa quando riceve un messaggio o una notifica;
2. sembra a disagio nell'andare a scuola o finge di essere malata (ha spesso mal di stomaco o mal di testa);
3. cambia comportamento ed atteggiamento in modo repentino;
4. mostra ritrosia nel dare informazioni su ciò che fa online;
5. soprattutto dopo essere stata online, mostra rabbia o si sente depressa;
6. inizia ad utilizzare sempre meno pc e telefono (arrivando ad evitarli);
7. perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;
8. il suo rendimento scolastico peggiora.

Cosa fa la scuola per prevenirlo?

AZIONI

A tal proposito verranno attivati dei percorsi formativi di prevenzione e conoscenza del fenomeno a tutti i livelli della comunictà scolastica nei prossimi anni.

Il tema verrà inserito all'interno del Piano dell'Offerta Formativa con la progettazione didattica e interdisciplinare propria del curricolo di Educazione Civica.

Un valido supporto nella nostra comunità è la psicologa della scuola, la quale, se necessario, può collaborare a costruire una pianificazione didattica (che può essere artistica, letteraria, teatrale, ecc..) in cui vengano previsti dei momenti di riflessione, brain storming, giochi di ruolo, partendo dalla programmazione didattica e a tal proposito si potranno utilizzare i video proposti da Generazioni connesse.

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.

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

"L'incitamento all'odio deve essere inteso, quindi, come comprensivo di tutte le forme di espressione che diffondono, incitano, promuovono o giustificano l'odio razziale, la xenofobia, l'antisemitismo o altre forme di odio generate dall'intolleranza, ivi comprese: l'intolleranza espressa dal nazionalismo e dall'etnocentrismo aggressivi, la discriminazione e l'ostilità nei confronti delle minoranze, dei migranti e delle persone con origine straniera" (www.coe.int). Tale fenomeno, purtroppo, negli ultimi anni si è fortemente diffuso e rafforzato soprattutto attraverso l'uso della Rete, e dei social network in particolar modo, dove non è difficile e infrequente trovare forme di odio e hate speech online particolarmente violente. Per questo è estremamente importante affrontarlo con ragazze e ragazzi anche a scuola.

AZIONI

Cosa fa la scuola per prevenirlo?

Nell'ottica della valorizzazione dell'esistente, si lavora a tal scopo tramite l'attività del Manifesto della Comunicazione Non Ostile proposto a tutte le prime in occasione dell'accoglienza.

Inoltre, le attività curricolari proprie dell'Educazione Civica sono volte al superamento di pregiudizi e stereotipi.

Anche il Gruppo Noi lavora su questa tematica, spiegando il fenomeno e offrendo spazi di discussione. Un utile spunto viene offerto dalla letteratura e dalla storia. Si propone la visione di video di generazioni connesse e la creazione di power point da condividere tra pari.

Un' ulteriore possibilità (compatibilmente con la situazione sanitaria emergenziale) è rappresentata da conferenze tenute da esperti esterni sui pregiudizi e gli stereotipi legati alla razza, genere, orientamento sessuale e all'accettazione del diverso, con il fine di fornire agli studenti gli strumenti necessari per decostruire stereotipi su cui spesso si fondano forme di hate speech.

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?

4.4 DIPENDENZA DA INTERNET E GIOCO ON LINE

Questa dipendenza nasce da un vero abuso della tecnologia anche denominato "Internet addiction Disorder", che è spesso correlato al Net gaming addiction o Internet gaming addiction ossia dipendenza dal gioco on line, una vera e propria patologia inserita all'interno del Manuale Diagnostico Statistico dei Disturbi Mentali (DSM5).

Va specificato che la dipendenza si realizza quando c'è un abuso, ossia un utilizzo continuativo e sistematico della Rete al fine di giocare impegnando la maggior parte delle giornate, con la conseguente sottrazione del tempo alle altre attività quotidiane del minore.

In particolare, sei sono le componenti che a livello bio-psico-sociale possono portare ad una vera e propria dipendenza. Di seguito i sintomi che devono essere presenti (per un arco di tempo di almeno un anno):

1. il giocatore è assorbito totalmente dal gioco;
2. il giocatore è preoccupato e ossessionato dal gioco (si veda Lancini M., Il ritiro sociale negli adolescenti, Raffaello Cortina Ed., Milano, 2019);
3. il gioco consente alla persona di sfuggire alla realtà con la sperimentazione di emozioni più piacevoli;
4. il giocatore manifesta sempre di più l'impulso di giocare e di sperimentare emozioni positive;
5. il giocatore sente di dover dedicare più tempo ai giochi;
6. il giocatore se non può giocare manifesta ansia, depressione e irritabilità;
7. può emergere un ritiro sociale;
8. il giocatore, anche se comprende la gravità della situazione e sospende di giocare, comunque non riesce a interrompere del tutto;
9. il giocatore mente agli altri sull'utilizzo che fa dei giochi on line;
10. il giocatore ha perso o mette a rischio relazioni o opportunità a causa dei giochi su Internet o ha perso interesse verso attività nella vita reale.

AZIONI

La scuola attraverso lo sviluppo delle competenze di cittadinanza digitale fa riflettere sull'uso critico della tecnologia e sul tempo dedicato ad essa. Indica strategie per un uso più consapevole delle tecnologie per favorire il "benessere digitale", cioè la capacità di creare e mantenere una relazione sana con la tecnologia.

In casi gravi la psicologa della scuola con la DS contatterà la famiglia e la indirizzerà verso un percorso riabilitativo da dipendenza con esperti esterni territoriali di riferimento.

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.

4.5 SEXTING

"Secondo una recente ricerca di Skuola.net per la Polizia di Stato - ricerca che ha coinvolto 6.500 ragazzi tra i 13 e i 18 anni - il 24% di loro ha scambiato almeno una volta immagini intime con il partner via chat o social (fenomeno conosciuto come sexting). Tra questi, il 15% ha subito la

condivisione con terzi, senza consenso, di questo materiale. Il motivo più frequente, riportato dalle vittime? Un banale "scherzo" (49%), a dimostrazione di quanto possano essere sottovalutate le reali conseguenze di tale diffusione. Tra le altre motivazioni, il ricatto (11%) o la vendetta (7%): il revenge porn, pure presente, viene surclassato dalla leggerezza e dalla goliardia ma gli effetti sono drammaticamente gli stessi. La reazione più diffusa nella maggior parte dei casi è il silenzio: il 53% ha fatto finta di niente, il 31% non ha detto nulla per non essere giudicato".

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

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

I contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di "revenge porn" letteralmente "vendetta porno" fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte (la Legge 19 luglio 2019 n. 69, all'articolo 10 ha introdotto in Italia il reato di revenge porn, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti. Si veda l'articolo 612 ter del codice penale rubricato "Diffusione illecita di immagini o video sessualmente espliciti".

Tra le caratteristiche del fenomeno vi sono principalmente:

1. la fiducia tradita: chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo, inoltre, alla motivazione della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale);
2. la pervasività con cui si diffondono i contenuti: in pochi istanti e attraverso una condivisione che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso a un numero esponenziale e infinito di persone e ad altrettante piattaforme differenti. Il contenuto, così, diventa facilmente modificabile, scaricabile e condivisibile e la sua trasmissione è incontrollabile;
3. la persistenza del fenomeno: il materiale pubblicato online può permanervi per un tempo illimitato e potrebbe non essere mai definitivamente rimosso. Un contenuto ricevuto, infatti, può essere salvato, a sua volta re-inoltrato oppure condiviso su piattaforme diverse da quelle originarie e/o in epoche successive.

La consapevolezza, o comunque la sola idea di diffusione di contenuti personali, si replica nel tempo e può finire con il danneggiare, sia in termini psicologici che sociali, sia il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che hanno contribuito a diffonderla. Due agiti, quindi, che sono fra loro strettamente legati e che rappresentano veri e propri comportamenti criminali i quali hanno ripercussioni negative sulla vittima in termini di autostima, di credibilità, di reputazione sociale off e on line. A ciò si associano altri comportamenti a rischio, di tipo sessuale ma anche

riferibili ad abuso di sostanze o di alcool.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/i e depressione.

AZIONI

La scuola ha tenuto con il Nucleo di Prossimità dei percorsi di prevenzione ed informativi.

La scuola ha siglato con il Comune di Novara e con il Nucleo di Prossimità della Polizia Locale un protocollo di intesa per la formazione degli alunni in prevenzione di qualsiasi forma di prevaricazione. In tale ambito si svolgono anche percorsi di prevenzione del sexting. Anche il Gruppo Noi discute di questa tematica e della pedopornografia.

Nel caso si presentasse il caso, la DS, il referente del cyberbullismo, il team preposto e la psicologa individueranno di volta in volta strategie mirate ed utili per affrontare il problema chiedendo il supporto delle famiglie e della polizia postale.

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.

4.6 ADESCAMENTO ON LINE

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 ad 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.

Potenziali vittime dell'adescamento online possono essere sia bambini che bambine, sia ragazzi che ragazze. Il fenomeno, infatti, non conosce distinzione di genere. Gli adolescenti sono particolarmente vulnerabili, poiché si trovano in una fase della loro vita in cui è molto importante il processo di costruzione dell'identità sessuale. Anche per questo potrebbero essere aperti e curiosi verso nuove esperienze e, talvolta, attratti da relazioni intime e apparentemente rassicuranti. In questa fase è importante, infatti, il bisogno di avere attenzioni esclusive da un'altra persona, di ottenere rinforzi esterni di approvazione per il proprio corpo e la propria immagine. È proprio in ragione della fiducia costruita nella relazione che le vittime di adescamento online riferiscono di sentirsi umiliate, usate, tradite e tendono a sentirsi in colpa e ad autosvalutarsi per essere cadute nella trappola.

L'adescamento, quindi, non avviene apparentemente con una dinamica violenta, ma il "prendersi cura" del minore rappresenta la conditio per carpirne la fiducia ed instaurare una relazione a sfondo erotico. Può capitare che l'adescatore si presenti al minore sotto falsa identità, fingendo quindi di essere un'altra persona così da attirare maggiormente l'attenzione del minore (ad esempio, potrebbe fingersi un talent scout del mondo dello spettacolo alla ricerca di volti nuovi).

Secondo una ricerca condotta da Ipsos per Save the Children Italia (2017) dal titolo "Che genere di tecnologie. Ragazze e digitale fra opportunità e rischi", il 42% delle ragazze fra i 12 e i 17 anni chatta spesso/sempre con qualcuno conosciuto in Internet e il 14,5% scopre che qualcuno con cui si è entrati in contatto in Internet non era la persona che diceva di essere. Piuttosto preoccupanti, inoltre, i dati sull'opinione delle ragazze fra i 12 e i 17 anni in relazione alla condivisione di materiale intimo e riservato online, destinato a rimanere fra una cerchia ristretta di persone.

Il 25,9% delle ragazze pensa che "è sempre sicuro, tanto lo fanno tutti", mentre il 40,3% pensa che "anche se non è sicuro, a volte non hai scelta".

AZIONI

Il nucleo di prossimità ha tenuto degli interventi, di prevenzione universale sulla tematica, in tutte le classi del biennio legati al rischio della rete. La Polizia Postale ha tenuto due interventi: spiegando le fasi dell'adescamento e il processo, ha dato ai ragazzi i riferimenti normativi e ha spiegato come intervenire se si sospetta o si ha la certezza di un caso di adescamento.

Nei prossimi anni verrà proposta, a seguito degli interventi degli esperti, una discussione partendo dai video interattivi proposti da Generazioni connesse a tal proposito.

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.

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 coinvolte/i in comportamenti sessualmente espliciti, concrete o simulate o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

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

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

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

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. Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia. L'intento è quello di facilitare il processo di rimozione del materiale stesso dalla Rete e allo stesso tempo consentire le opportune attività investigative finalizzate ad identificare chi possiede quel materiale, chi lo diffonde e chi lo produce, ma, soprattutto e primariamente, ad identificare i minori abusati presenti nelle immagini e video, assicurando la fine di un abuso che potrebbe essere ancora in corso e il supporto necessario.

Parallelamente, se si ravvisa un rischio per il benessere psicofisico dei/lle bambini/e, ragazzi/e

coinvolte 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.

Se si è a conoscenza di tale tipologia di reato è possibile far riferimento alla: Polizia di Stato – Compartimento di Polizia postale e delle Comunicazioni; Polizia di Stato – Questura o Commissariato di P.S. del territorio di competenza; Arma dei Carabinieri – Comando Provinciale o Stazione del territorio di competenza; Polizia di Stato – Commissariato online

Per questo motivo, nella nostra scuola l'educazione, compresa l'educazione all'affettività, riveste un ruolo fondamentale.

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.

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

□ 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.

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.

5.1 COSA SEGNALARE

In riferimento al cyberbullismo si potrebbero palesare i seguenti casi:

CASO A (SOSPETTO): il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/studentesse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting, o adescamento on line.

CASO B (SOSPETTO): gli studenti/studentesse, i peer, il personale ATA hanno il sospetto che stia avvenendo qualcosa tra gli/le studenti/studentesse della propria scuola, riferibile a un episodio di bullismo e/o cyberbullismo, sexting, o adescamento on line.

CASO C (SOSPETTO): i genitori hanno il sospetto che stia avvenendo qualcosa al proprio figlio/figlia, riferibile a un episodio di bullismo e/o cyberbullismo, sexting, o adescamento on line.

CASO D (EVIDENZA): il docente ha evidenze certa che stia accadendo qualcosa tra gli/le studenti/studentesse della propria classe

CASO E: gli studenti/studentesse, i peer, il personale ATA hanno evidenza certa che stia accadendo qualcosa tra gli/le studenti/studentesse della propria scuola, riferibile a un episodio di bullismo e/o cyberbullismo, sexting, o adescamento on line.

CASO F: i genitori hanno evidenza certa che stia avvenendo qualcosa al proprio figlio/figlia, riferibile a un episodio di bullismo e/o cyberbullismo, sexting, o adescamento on line.

Nel caso A-B-C la procedura prevede:

1. prima segnalazione attraverso sportello Generazioni connesse
2. Intervento entro 24 ore del referente al bullismo e cyberbullismo e presa in carico del caso
3. Valutazione approfondita
4. Gestione del caso e interventi
5. Codice verde: situazione da monitorare con interventi preventivi nella classe (coinvolti nella scuola: DS, referente cyberbullismo, docenti della classe/consiglio di classe, operatori scolastici)
6. Possibilità di segnalare al garante della privacy eventuali contenuti offensivi/lesivi che li riguardano
7. Monitoraggio dell’efficacia degli interventi

Nel caso D-E-F

1. Prima segnalazione attraverso lo sportello Generazioni connesse
2. Intervento entro 24 ore del referente al bullismo e cyberbullismo e presa in carico del caso
3. Valutazione approfondita (Ds, team, psicologa della scuola
4. Gestione del caso e valutazione della sofferenza della vittima: due interventi
5. Codice giallo/interventi indicati: approccio educativo con la classe, approccio individuale (con

la psicologa della scuola), gestione della relazione, coinvolgimento della famiglia (coinvolti nella scuola: DS, docenti della classe, referente cyberbullismo, polizia postale, genitori)

6. Possibile ammonimento del questore: l'ammonimento è uno strumento di prevenzione, volto ad evitare il coinvolgimento del minore, sia quale autore del reato sia quale vittima, in procedimenti penali.

L'istanza di ammonimento nei confronti del minore ultraquattordicenne, autore di atti di cyberbullismo, va rivolta al Questore.

È possibile ricorrere all'ammonimento soltanto nel caso in cui non vi siano reati perseguibili d'ufficio o non sia stata formalizzata querela o presentata denuncia per le condotte di ingiuria (reato depenalizzato), diffamazione, minaccia o trattamento illecito dei dati personali, commessi mediante la rete Internet nei confronti di un altro minorenne.

La richiesta può essere presentata ad un qualsiasi ufficio di Polizia e deve contenere una dettagliata descrizione dei fatti, delle persone a qualunque titolo coinvolte ed eventuali allegati comprovanti quanto esposto.

Se l'istanza è ritenuta fondata, anche a seguito di approfondimenti investigativi, il Questore convoca il minore responsabile insieme ad almeno un genitore o ad altra persona esercente la potestà genitoriale; procede quindi ad ammonire oralmente il minore, invitandolo a tenere una condotta conforme alla legge con specifiche prescrizioni che varieranno in base ai casi.

Gli effetti dell'ammonimento cessano al compimento della maggiore età.

7. Monitoraggio dell'efficacia degli interventi

8. Codice rosso/interventi di emergenza: intervento individuale (da parte della psicologa della scuola), coinvolgimento della famiglia (da parte del DS e del team), della polizia postale, supporto intensivo al lungo termine e rete (da parte del DS, team, che dovranno coinvolgere la famiglia e fornire l'accesso alla rete)

Monitoraggio dell'efficacia degli interventi

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.

5.2 COME SEGNALARE: QUALI STRUMENTI E A CHI

A chi segnalare:

1. sportello Generazioni connesse
2. referente bullismo-cyberbullismo
3. e mail apposita per le segnalazioni all'interno dell'area del sito della scuola denominata "Generazioni connesse"

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.

5.3 GLI ATTORI SUL TERRITORIO

Polizia Postale e delle comunicazioni

Nucleo di prossimità

Helpline Telefono azzurro (19696)

Comitato Regionale Unicef: difensore dei diritti dell'infanzia

Co.Re.Com (Comitato regionale per le comunicazioni)

Ufficio Scolastico Regionale: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet

Aziende Sanitarie Locali

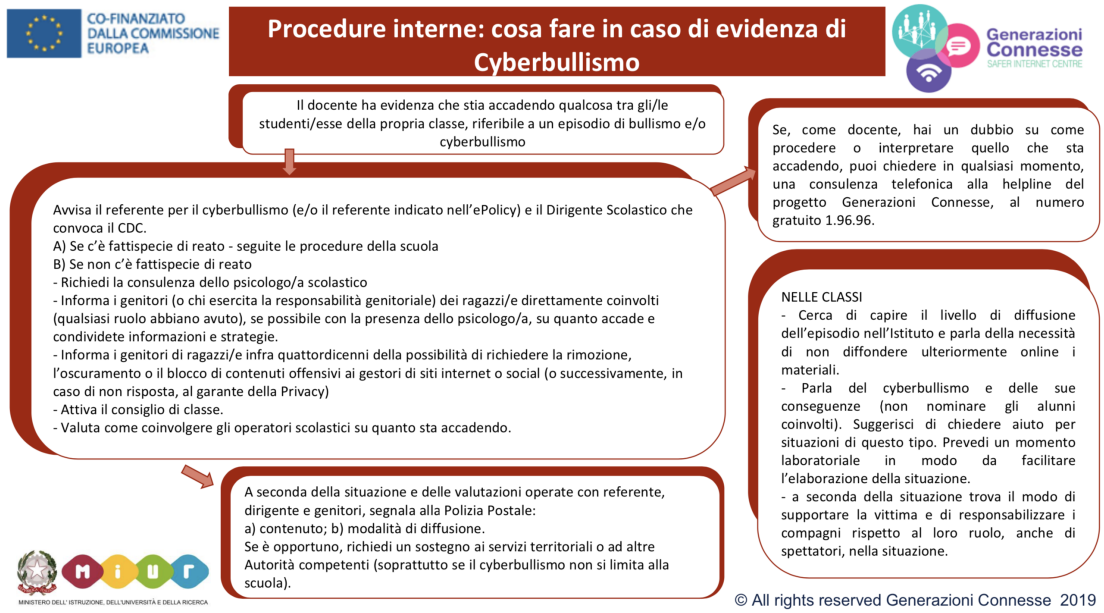
Garante regionale per l'infanzia e l'Adolescenza e Difensore Civico

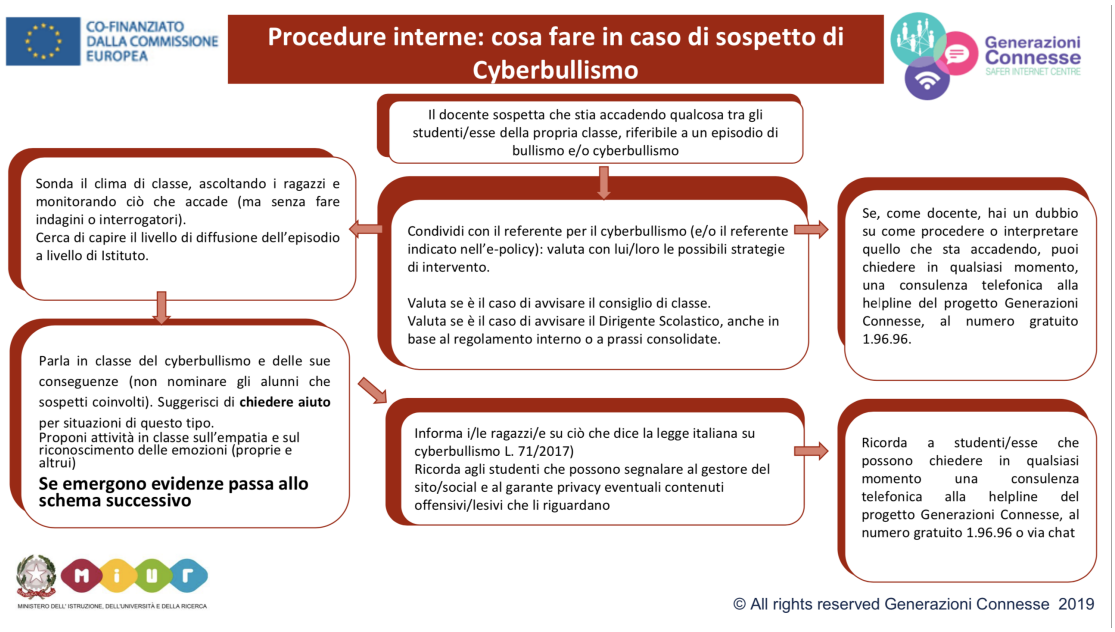
Tribunale per i minorenni

Sul sito della scuola nella sezione "Generazioni connesse" 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".

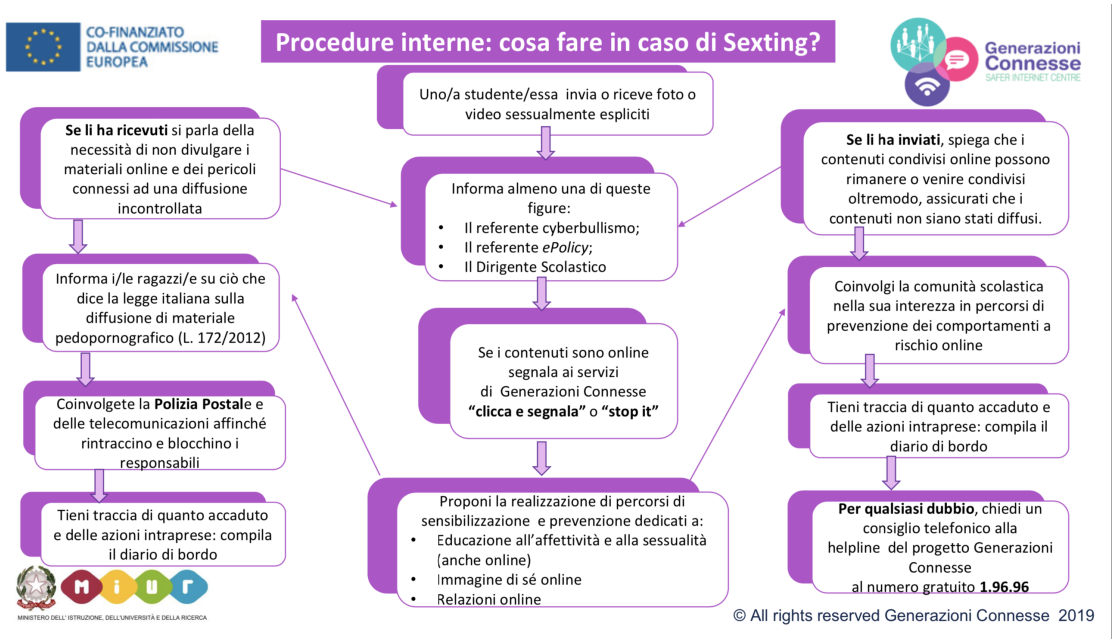
5.4. - Allegati con le procedure

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

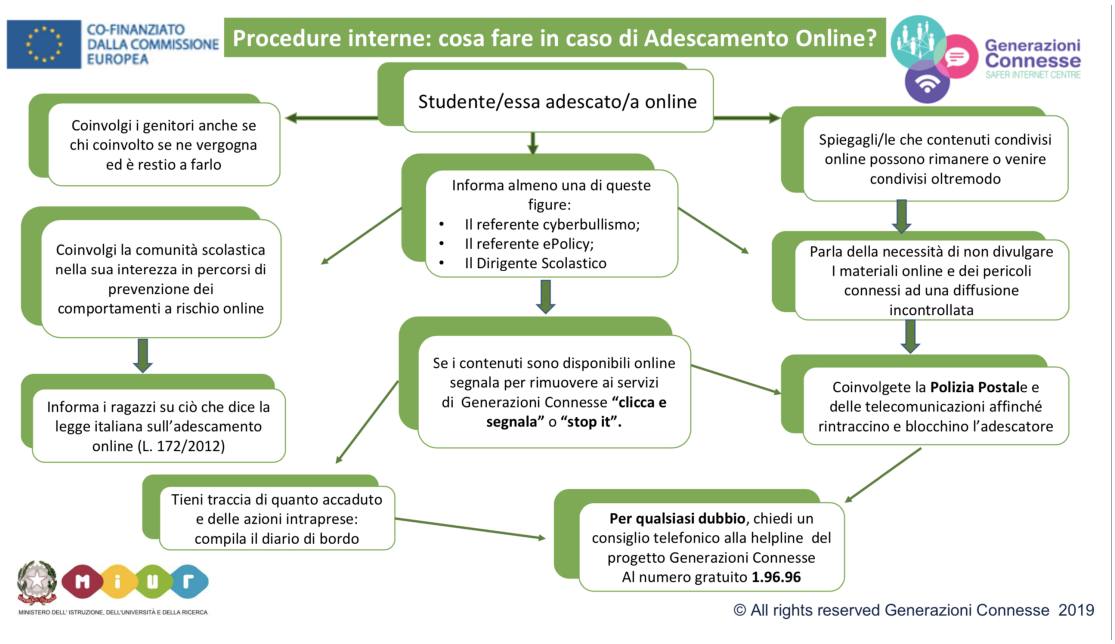




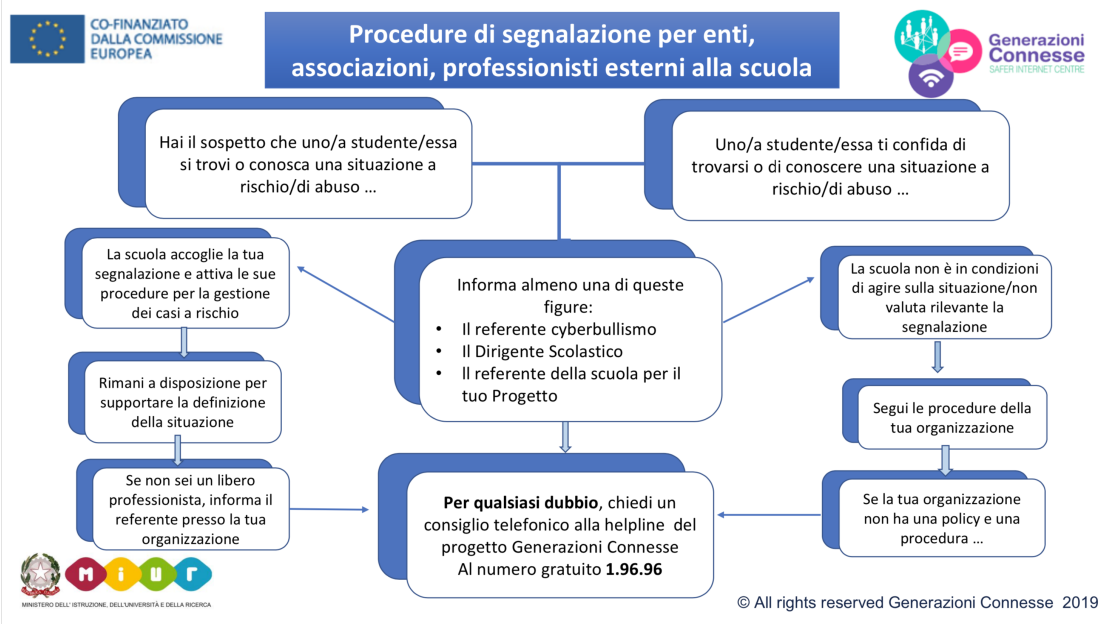
Procedure interne: cosa fare in caso di sexting?



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

Il nostro piano d'azioni

Non è prevista nessuna azione.