Documento di ePolicy

NAIC8C000R
T.GRECOI.C. GIACOMO LEOPARDI
VIA COM.TE G.B. DELLA GATTA 2 - 80059
TORRE DEL GRECO - NAPOLI (NA)

www.icleopardi.edu.it

Dirigente Scolastico Prof.ssa Olimpia Tedeschi

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 per l'apprendimento degli studenti e delle studentesse.

Le "competenze digitali" sono abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente vanno acquisite 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, ossia un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia nei ragazzi e nelle ragazze che negli 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 tecnologici.

Il presente documento ha l'obiettivo di esprimere la visione educativa e la conseguente proposta formativa dell'I.C. Giacomo Leopardi di Torre del Greco, in riferimento alle tecnologie digitali.

Nello specifico esplicita:

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 relative a comportamenti on-line a rischio;

le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

Argomenti del Documento

Perché è importante dotarsi di una e-policy?

Attraverso l'e-policy il nostro Istituto Comprensivo si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento per assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, 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 "ben essere" in Rete, definendo le regole di utilizzo delle TIC a scuola e pone le basi per azioni formative e educative su e con le tecnologie digitali, da usare in modo consapevole e responsabile.

1.2 - Ruoli e responsabilità

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

La scuola, nel farsi carico della formazione globale dell'individuo nella sua delicata fase evolutiva, deve individuare in maniera chiara e inequivocabile i ruoli e le responsabilità di ciascuno degli attori coinvolti nel percorso formativo. Nella promozione dell'uso consapevole della rete esistono compiti peculiari:

Il **Dirigente Scolastico** deve:

- garantire la corretta formazione del personale scolastico sulle tematiche relative all'uso sicuro e consapevole di Internet e della rete;
- garantire una formazione adeguata del personale docente relativo all'uso delle TIC nella didattica;
- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di Internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;
- seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.
- Promuovere il contrasto ad ogni forma di disagio, illegalità, bullismo, mettendo in campo azioni e strategie per prevenirlo.

L'**Animatore digitale**, supportato dal **Team dell'innovazione**, deve:

- stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale";
- fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali;
- proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate;
- curare la manutenzione e lo sviluppo del sito web della scuola utilizzato per scopi istituzionali e consentiti (istruzione, comunicazione, formazione, promozione e valorizzazione delle attività progettuali);
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti alla "scuola digitale".

Il **referente del bullismo e cyberbullismo** deve:

- coordinare e socializzare iniziative specifiche per la prevenzione ed il contrasto al bullismo e cyberbullismo, in accordo con il Dirigente, avvalendosi della collaborazione delle Forze di polizia, Associazioni e centri di aggregazione giovanile del territorio o e carattere nazionale con cui la scuola avrà stipulato partenariati e/o convenzioni;
- coinvolgere nei progetti e nei percorsi formativi deliberati, studenti, genitori e personale scolastico.

Il **Direttore dei servizi generali e amministrativi** deve:

- assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;
- operare per il buon funzionamento dei diversi canali di comunicazione della scuola (circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di Internet;
- vigilare che venga sottoscritta nei contratti con enti, esperti ed associazioni operanti nella scuola la presa visone del documento di e-policy d'istituto.

I Docenti devono:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di Internet e sulla politica di sicurezza assunta dalla scuola, rispettando il regolamento;
- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di Internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- operare perché gli alunni comprendano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di Internet;
- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete, ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali e trasparenti;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica deliberata;
- indirizzare gli alunni all'utilizzo di internet su siti adeguati ai fini didattici utilizzando e facendo utilizzare nel caso di visione di filmati, esclusivamente piattaforme legali: *Youtube*, *Netflix*, *Dzon* e similari. (È fatto divieto assoluto di utilizzare piattaforme streaming video perché illegali e pericolose per contagio da malware del pc _ lim di classe);
- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni, ovvero valutazioni sulla condotta non adeguata degli stessi rilevati a scuola, in rapporto all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo all'Animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola, utili ad aggiornamento costante della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- segnalare al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di Internet, per l'adozione delle procedure previste dalle norme.

Gli Alunni devono:

- essere responsabili, in relazione al proprio grado di maturità e di apprendimento, nell'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti e dalle regola vigenti;
- avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali, ma anche comprendere la necessità di evitare il plagio e rispettare i diritti d'autore;
- adottare le buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali così da non correre rischi;
- assumere condotte rispettose degli altri anche quando si comunica in rete (vedi "Comunicazione non ostile");
- esprimere domande, difficoltà e bisogno di aiuto nell'utilizzo delle tecnologie didattiche e di Internet ai docenti e ai genitori.

I Genitori devono:

- sostenere la linea di condotta che la scuola ha deliberato nei confronti dell'utilizzo delle TIC nella didattica;
- seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti e dal regolamento scolastico;
- relazionarsi in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete e comunicare con loro circa i problemi rilevati quando i figli non usano responsabilmente le tecnologie digitali o Internet;
- fissare anche a casa tempi e regole per l'utilizzo del computer e vigilare sull'uso che i figli quotidianamente fanno di Internet e dei *devices* (PC, cellulari, tablet ecc.);
- accettare e condividere quanto scritto nell'e-policy dell'Istituto.
- Gli Enti esterni e le Associazioni impegnate in partenariato e convenzioni con l'I.C. Giacomo Leopardi di Torre del Greco devono:

- conformarsi alla politica della scuola riguardo l'uso consapevole delle TIC e della Rete, nel rispetto del regolamento vigente;
- promuovere ed applicare la sicurezza online, assicurando la protezione degli studenti durante le attività che svolgono con loro.

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

Tutti gli attori che sono interessati ad entrare in relazione educativa con gli studenti e le studentesse dell'I.C. Giacomo Leopardi, devono mantenere sempre un elevato profilo personale e professionale, bandendo atteggiamenti inappropriati, ed essere guidati dal principio dell'interesse superiore e della salvaguardia assoluta del minore.

Sono vietati comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse, con obbligo di denuncia al dirigente, e vanno prevenuti , contrastati e denunciati al Dirigente, comportamenti di minori illegali e scorretti o che mettano a rischio la loro sicurezza.

Tutti gli attori esterni sono tenuti a conoscere e a rispettare il regolamento del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e di 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), per il cui uso è necessaria una specifica autorizzazione scritta da parte dei genitori.

Le organizzazioni/associazioni extrascolastiche e gli esperti esterni chiamati a vario titolo, alla realizzazione di progetti ed attività educative sul breve o/e lungo periodo, dovranno prendere atto di quanto stilato nell' e-policy dell'Istituto e sottoscrivere la presa visione del documento in questione, all'atto del contratto.

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

Il documento di e-Policy è condiviso con tutta la comunità educante, esso pone al centro gli studenti e le studentesse sottolineando i compiti, le funzioni e le responsabilità di tutti gli attori coinvolti nel processo educativo ed organizzativo. È molto importante pertanto che ciascun attore si faccia a sua volta promotore responsabile del documento. La condivisione del documento di e-Policy e la conoscenza dei suoi contenuti sono promossi attraverso:

- la socializzazione nelle sedi collegiali;
- la pubblicazione del documento sul sito istituzionale della scuola;
- la stipula del Patto di Corresponsabilità sottoscritto dalle famiglie all'inizio dell'anno scolastico.

Il documento approvato dal Collegio dei Docenti e dal Consiglio di Istituto e pubblicato sul sito, viene altresì esposto anche fisicamente nei tre plessi del comprensivo. All'interno del documento di e-Policy è inglobato ove prevista la e-Safety Policy:

Gli alunni:

- saranno informati che la rete e la navigazione in Internet attraverso i vari dispositivi digitali saranno controllati dagli insegnanti e che andranno utilizzati solo previa loro autorizzazione;
- si impegneranno nell'uso responsabile e sicuro di Internet (come attività propedeutica all'accesso nella rete);
- prenderanno visione delle regole per la sicurezza on-line pubblicate nelle aule e nei laboratori con accesso a Internet;
- saranno formati in rapporto alla sicurezza e ai pericoli a cui sono più esposti e pertanto dovranno assumere atteggiamenti consapevoli e responsabili.

I docenti:

- devono conoscere le linee di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di Internet, contenute nel presente documento e tutto il materiale informativo pubblicato, a corredo, sul sito web della scuola;
- dovranno utilizzare e far utilizzare tutti gli strumenti digitali esclusivamente in rapporto alle esigenze didattiche deliberate;
- aver coscienza che il traffico in Internet è monitorato e pertanto si potrà risalire al singolo utente registrato;
- dovranno informarsi e formarsi nell'uso sicuro e responsabile di Internet, anche partecipando alle iniziative formative all'uopo deliberate.

Si precisa che:

il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC (Firewall) sarà supervisionato dal collaboratore tecnico, che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi tecnici;

l'Animatore digitale metterà in evidenza on-line utili strumenti che il personale potrà usare con gli alunni in classe, a seconda dell'età e della capacità connessa all'età e al grado scolare dei minori;

tutto il personale deve essere consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

L'**Animatore digitale** fornirà ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di Internet anche a casa grazie all'attivazione dello Sportello digitale; l'utente potrà prenotare il servizio attraverso il sito.

L'Animatore digitale e i docenti di classe forniranno ai genitori eventuali indirizzi web relativi a risorse utili per lo studio e a siti educativi da cui i minori potranno attingere a materiali utili e non pericolosi.

1.5 - Gestione delle infrazioni alla ePolicy

La scuola, nell'azione di controllo e monitoraggio a cui è demandata, gestirà le infrazioni all'e-policy attraverso interventi educativi specifici e, qualora fosse necessario, ricorrendo alle sanzioni previste in rapporto ai diversi gradi di gravità delle violazioni.

Le potenziali infrazioni in cui è possibile che gli alunni incorrano nell'uso della tecnologia digitale e di Internet sono connesse a queste tipologie di comportamenti scorretti:

- l'uso della rete e dei social al fine di criticare, infastidire e oltrepassare gli altri per ostacolarne la partecipazione;
- l'invio incauto di foto, video, informazioni o dati personali come l'indirizzo di casa, il telefono o la condivisione di immagini intime;
- la comunicazione incauta con sconosciuti;
- il collegamento a siti web non autorizzati dai docenti.

Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo dell'alunno: più gli alunni sono piccoli, più i comportamenti "da correggere" sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie; essi devono devono essere orientati dagli educatori nella prospettiva del raggiungimento di una maggiore consapevolezza e maturità.

I provvedimenti "disciplinari" proporzionati all'età ed alla gravità del comportamento previsti nel regolamento deliberato dalla scuola sono:

- il richiamo verbale;
- il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);
- il richiamo scritto con annotazione sul diario e il registro elettronico;
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente scolastico.

Contestualmente sono previsti da parte della scuola interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, quali:

- ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe;
- prevenzione e gestione positiva dei conflitti;
- moderazione dell'eccessiva competitività;
- promozione di rapporti amicali e di reti di solidarietà;
- promozione della conoscenza e della gestione delle emozioni.

Disciplina del personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico incorra nell'utilizzo delle tecnologie digitali e di Internet sono diverse. Alcune possono determinare, favorire o avere conseguenze dirette di maggiore o minore rilievo, sull'uso corretto e responsabile delle TIC da parte degli alunni.

Ecco quello che è necessario evitare:

- un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- una carente istruzione preventiva degli alunni sull'utilizzazione corretta e responsabile delle tecnologie digitali e di Internet;

- una vigilanza elusa degli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;

insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.

Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a Internet, la posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone una copia per eventuali successive investigazioni.

Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo, gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

Disciplina dei genitori

In considerazione dell'età degli alunni e della loro dipendenza dagli adulti, appare evidente che anche alcune situazioni possono favorire o meno l'uso corretto e responsabile delle TIC a scuola. I genitori, pertanto, sono invitati a vigilare affinché non si verifichino condizioni di rischio che i minori non possono e non sanno gestire.

Situazioni e condizioni che generano rischi per i minori:

- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai;
- la collocazione del computer/tablet/device in una stanza o in un posto non controllabile quando è utilizzato dal proprio figlio;
- concedere la piena autonomia al proprio figlio minore nella navigazione sul web e nell'utilizzo del PC, del cellulare, dello smartphone e dei social;
- un utilizzo del pc in comune con gli adulti. Tali devices possono conservare in memoria materiali non idonei;
- un utilizzo eccessivo ed illimitato nel tempo delle connessioni;
- un utilizzo dei social-network non consentito dalla legge europea sulla privacy. Va ricordato all'uopo che il GDPR indica i sedici anni come l'età minima per dare il proprio consenso digitale, cioè scegliere autonomamente di iscriversi a un Social Network.

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse, ricordando che sono responsabili a norma di legge, in base alla gravità dei comportamenti dei loro figli minorenni, qualora questi dovessero risultare pericolosi per sé e/o dannosi per gli altri.

1.6 - Integrazione dell'ePolicy e complementarietà con i Regolamenti esistenti nella scuola

Si ricorda che il Regolamento dell'Istituto scolastico adottato dall'istituto va rispettato da tutta la comunità scolastica e l'utenza che si relaziona con la realtà scolastica. Esso, essendo un documento di fondamentale importanza, viene periodicamente aggiornato dagli organi competenti per essere in sintonia con la realtà che la comunità scolastica vive. Esso è collegato strettamente al presente documento di e- policy e al il Patto di Corresponsabilità (sottoscritto anche dai genitori), che da questi atti deriva, in coerenza con le Linee Guida Miur e le indicazioni normative generali che interessano il mondo della scuola.

A tal proposito si richiamano in particolare l'Art. 28 del Regolamento d'istituto (Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del bullismo e del cyberbullismo), arricchito con l'indicazione del referente per le attività di prevenzione e di contrasto al bullismo ed al cyberbullismo, secondo le indicazioni ministeriali; e l'Art. 29 (Sanzioni disciplinari ed organi competenti all'erogazione del provvedimento), in cui è stata aggiunta una sezione relativa ai comportamenti sanzionabili e ai provvedimenti riguardanti l'uso non corretto della strumentazione personale e di qualsiasi dispositivo elettronico durante l'orario scolastico. Tale sezione contempla, inoltre, le procedure operative da adottare negli eventuali casi di cyberbullismo. All'Art. 88 si evidenziano le regole da rispettare per l'accesso ai laboratori di informatica e il loro corretto utilizzo. Alla luce dell'e-Policy è stato altresì integrato il Patto di Corresponsabilità (allegato nel Regolamento d'Istituto) che è un documento fondamentale nell'ambito del rapporto sinergico scuola/famiglia.

1.7 - Monitoraggio dell'implementazione della e-Policy e suo aggiornamento

Il documento di e-Policy è "dinamico", come lo è la vita della scuola e pertanto viene aggiornato allorquando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno dell'istituzione scolastica. Le modifiche del documento vanno sempre deliberate dagli organi collegiali. Il monitoraggio del documento è realizzato periodicamente, a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici posti e descritti al suo interno.

Il monitoraggio dell'implementazione della Policy e del suo eventuale aggiornamento sarà curato dal Dirigente Scolastico con la collaborazione dell'Animatore digitale, del Team digitale e del referente del bullismo e cyberbullismo. Avrà il fine di rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di Internet.

Il monitoraggio on-line sarà rivolto anche ai docenti, al fine di valutare l'impatto della Policy e la necessità di eventuali miglioramenti. L'aggiornamento della Policy sarà curato dal Dirigente scolastico, dall'Animatore digitale, dal Team, dal responsabile del bullismo e cyberbullismo e deliberato dagli Organi Collegiali.

Il nostro piano d'azioni

Il nostro Istituto comprensivo per far conoscere all'utenza il documento di e-Policy, si è posto degli obiettivi da raggiungere a breve, medio e lungo termine, qui di seguito indicati:

Azioni da svolgere entro un'annualità scolastica:

- Pubblicare sul sito della scuola il documento deliberato dagli organi collegiali, con la pagina di presentazione del progetto Generazioni Connesse, ad esso associato, rivolto agli studenti, ai docenti ed ai genitori. Detta pagina è il riferimento univoco per le attività seminariali svolte sulla piattaforma in rapporto al contrasto dei fenomeni del bullismo e cyberbullismo e per l'educazione all'uso responsabile della tecnologia e dei media.

Azioni da svolgere nei prossimi 3 anni:

- Presentazione dell' e-Policy agli studenti e ai genitori delle classi in ingresso, mediante incontri in presenza ed online. Approfondimento dei temi trattati.

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

Nella società odierna, i ragazzi, definiti "nativi digitali", usano la Rete pressoché quotidianamente, essendo ormai la tecnologia entrata prepotentemente nelle vite di tutti e nelle dinamiche sociali oltre che economiche. Essi, per quanto "intuitivamente" abili con i *devices*, mancano di quella necessaria consapevolezza che è espressione di maturità e che risulta essenziale per l'acquisizione delle cosiddette "competenze digitali".

Infatti, "la **competenza digitale**" presuppone l'interesse per le tecnologie digitali e il loro utilizzo non solo con dimestichezza, ma con spirito critico e responsabilità, aspetti che si acquisiscono mediante un'opportuna alfabetizzazione informatica e digitale che non può essere disciolta dall'educazione alla sicurezza informatica e, nello specifico della scuola, dalla cybersicurezza. ("Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente", C189/9, p.9).

Per questo l'Istituto comprensivo "**Giacomo Leopardi**" si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse ad un uso consapevole e responsabile delle tecnologie digitali. Ciò avviene ed avverrà gradualmente in maniera crescente,, attraverso la progettazione e l' implementazione del cosiddetto curricolo digitale .

L'Istituto Comprensivo "Giacomo Leopardi" si è dotato già nell'anno scolastico 2018-2019
di un curricolo trasversale per competenze in cui sono contemplate le competenza digitali, ritenute dall'Unione Europea competenze chiave trasversali alle discipline, così come previsto anche dalle Indicazioni Nazionali. Possedere competenze digitali significa , ad un tempo, padroneggiare le abilità e le tecniche di utilizzo delle nuove tecnologie, ma anche soprattutto utilizzarle con autonomia, responsabilità e con spirito critico, nel rispetto degli altri, sapendo prevenire ed evitare i pericoli e i rischi ad esse connessi. In questo senso, tutti gli insegnamenti e tutti i relativi docenti sono coinvolti nell'opera di promozione e costruzione di tali competenze digitali negli alunni, per cui, da professionisti, si impegnano in un processo continuo di formazione e di aggiornamento .
L'Istituto ha inoltre aderito a partire dall'a.s. 2015/2016 al progetto ministeriale "Programma il futuro" che ha coinvolto tutte le classi e le sezioni di tutti gli ordini scolari nella sperimentazione del coding (Code Week e l'ora del coding) e del pensiero computazionale, strettamente connesso all'acquisizione delle competenze digitali. Ha, inoltre, provveduto:

- all'attivazione di laboratori artistici con l'utilizzo di strumentazione digitale;
- alla creazione di un Atelier creativo, finanziato dal Ministero;

L' istituto ha altresì promosso eventi ed attività laboratoriali volti alla promozione dell'Educazione alla Cittadinanza attiva ed alla Legalità per educare gli alunni alla vita sociale ed al rispetto delle regole della convivenza democratica. Tra questi:

- laboratori digitali pomeridiani per l'uso consapevole delle tecnologie digitali;
- conferenze ed incontri seminariali sulla Costituzione;
- incontri formativi con psicologi e Polizia postale per la prevenzione ed il contrasto al bullismo e al cyberbullismo;
- convenzioni formative, a titolo non oneroso per la scuola, con il Tribunale di Torre Annunziata, l'Associazione Libera, Save the Children ed altri enti ed associazioni senza scopo di lucro, attive nel campo della Legalità;
- partecipazione degli alunni della Secondaria di primo grado al Safer Internet;
- visione di film e documentari su tematiche inerenti al bullismo ed al cyberbullismo per la Scuola Secondaria di I grado.

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 competente, trasversale ed inclusivo.

Ciò si rende necessario per fornire agli studenti e alle studentesse modelli positivi di utilizzo delle strumentazioni digitali, utili a favorire il miglioramento di tutto il processo di apprendimento.

A tale proposito, il comma 124 della Legge n. 107/2015 recita quanto segue: "Nell'ambito degli adempimenti connessi alla funzione docente, la formazione in servizio dei docenti di ruolo è obbligatoria, permanente e strutturale. Le attività di formazione sono definite dalle singole istituzioni scolastiche in coerenza con il Piano triennale dell'offerta formativa e con i risultati emersi dai piani di miglioramento delle istituzioni scolastiche previsti dal regolamento di cui al decreto del Presidente della Repubblica 28 marzo 2013, n. 80, sulla base delle priorità nazionali indicate nel Piano nazionale di formazione, adottato ogni tre anni con decreto del Ministro dell'istruzione, dell'università e della ricerca, sentite le organizzazioni sindacali rappresentative di categoria."

Pertanto dal 2015 ad oggi, il corpo docente ha partecipato costantemente a corsi di formazione promossi dalla scuola e dall'Ambito 21 di appartenenza, in sintonia con il PNSD. Infine negli ultimi due anni, in seguito alla situazione pandemica generata dalla diffusione del Covid 19, che ha reso necessaria l'attivazione di forme nuove di didattica a distanza (DAD, DDI), il corpo docente si è formato con specifici corsi nel settore digitale ed ha raggiunto generalmente una buona competenza di base. Tale competenza è diventata specialistica per alcune figure nate nel rinnovato orizzonte scolastico quali l'Animatore digitale ed i componenti del Team digitale. Il personale scolastico è, infine, disponibile ad aggiornarsi, in quanto ha chiaro che il percorso complesso della formazione nel settore delle TIC applicate alla didattica non si può esaurire in breve tempo, considerato il progresso galoppante delle tecnologie. Perciò sono previsti anche nel corso dell'attuale anno scolastico e di quelli a venire, momenti di auto aggiornamento, momenti di formazione personale e collettiva all'interno dell'Istituto, la condivisione delle conoscenze dei singoli, il supporto dell'Animatore digitale e del Team e l'eventuale partecipazione a corsi di aggiornamento online. Infine, l'Animatore digital sta lavorando per consentire al personale scolastico, agli studenti ed alle loro famiglie, la fruizione di materiali utili messi a disposizione e pubblicati in bacheche virtuali sul sito della scuola quali: manuali, guide e tutorial per la didattica con le TIC.

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

La scuola si impegna a promuovere anche nei prossimi anni scolastici, 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 verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (Animatore digitale, referente bullismo e cyberbullismo) e se necessario con l'ausilio di 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 ad hoc selezionate. L'Istituto Comprensivo "Giacomo Leopardi" , come già detto, si avvale da circa tre anni, della figura dell'Animatore digitale che collabora con il Dirigente Scolastico e il D.S.G.A. per la promozione e realizzazione gli obiettivi di innovazione deliberate nel PTOF della scuola, nell'ambito del PNSD. Inoltre, a partire dall'anno scolastico 2015-2016 è attiva la figura del Referente d'Istituto per le attività di prevenzione e contrasto al bullismo e al cyberbullismo (L.107/2015).

La formazione sull'utilizzo consapevole e sicuro delle TIC è stata estesa ad altre figure, in funzione della costituzione di un Team digitale per le emergenze. Si rende, comunque, necessaria la formazione permanente di tutti i docenti sull'uso consapevole e sicuro di Internet e sui rischi della rete in relazione all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono nel quotidiano e, spesso, in maniera autonoma, i ragazzi.

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

Nella prevenzione dei rischi connessi al mondo digitale così come nella promozione di un uso maturo e responsabile delle TIC, è necessaria la collaborazione di tutti gli attori educanti. Scuola e famiglia, come più volte ribadito, devono rafforzare anche in questo campo l'alleanza educativa e promuovere percorsi formativi condivisi, utili ai ragazzi/e e ai bambini/ anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie su tutte le attività e le iniziative intraprese sul tema delle tecnologie digitali previste dal documento di e-Policy, richamato nel "Patto di corresponsabilità" aggiornato e pubblicato sul sito web dell'Istituto. Scuola e famiglia sono chiamate a sottoscriverlo e a collaborare per garantire la crescita formativa di ciascun alunno. La sua stipula avviene all'inizio di ogni anno scolastico. L'Istituto attiverà nel corso dell'anno, iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine saranno previsti incontri fra docenti e/o esperti e genitori sui temi oggetto della Policy e per la diffusione del materiale informativo sulle tematiche trattate messo a disposizione dai siti specializzati (Generazioni Connesse), nonché incontri con la psicologa dello Sportello Ascolto e con le Forze dell'ordine. Sul sito della scuola, inoltre, sarà pubblicato il presente documento di e-Policy per la divulgazione delle informazioni e delle procedure contenute e saranno postati gli avvisi relativi a tutti gli incontri formativi/informativi.

Il nostro piano d'azioni

(da sviluppare nell'arco dell'anno scolastico 2021/2022)

Le azioni che la scuola si propone di realizzare nel corso dell'anno scolastico 2021/22 sono le seguenti:

- coinvolgere una rappresentanza dei genitori nella piattaforma "Generazioni connesse"per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale;
- promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica;
- adesione per docenti e studenti della Secondaria di primo grado al progetto "Percorsi per l'acquisizione di competenze per la cittadinanza digitale", progetto a cura di Save the Children con la supervisione dell'Università Cattolica di Milano.

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

Le azioni che la scuola si propone di realizzare nel corso dei prossimi anni sono le seguenti:

- attivazione, all'interno della scuola, di laboratori per l'acquisizione della patente europea;
- azione di monitoraggio e di programmazione delle attività svolte con il coinvolgimento dei genitori.

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 abitualmente trattati numerosi dati personali di docenti, ATA, studenti e relative famiglie. Talvolta, tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali e vanno trattati con cautela. Il "corretto trattamento dei dati personali" a scuola è, infatti, 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 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), ed è promosso dal Regolamento UE 2016/679, dal Parlamento europeo e dal Consiglio.

Le scuole, quindi, hanno 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 merito alla protezione dei dati personali, si fa riferimento a quanto previsto dal Decreto Legislativo del 30 giugno 2003, n.196 (cosiddetto Codice della Privacy), integrato dal D. Lgs. 10 agosto 2018, n. 101, e dal GDPR (*General Data Protection Regulation*) n. 679 del 2016.

In questo paragrafo dell'e-Policy 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 al presente documento di e-Policy, i modelli di liberatoria conformi alla normativa vigente, da utilizzare in materia di protezione dei dati personali.

All'atto dell'iscrizione, nella stessa domanda da redigere, viene fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei prodotti artistico-creativi degli alunni per la partecipazione a concorsi interni ed esterni, a mostre e manifestazioni culturali, e l'autorizzazione all'utilizzo di fotografie, video o altri materiali audiovisivi contenenti l'immagine e/o il nome del proprio figlio/a per scopi documentativi sull'operato della scuola o per la partecipazione a concorsi. A tale proposito si evidenzia che le immagini e le riprese audio- video realizzate dalla scuola, nonché gli elaborati e I manufatti prodotti dagli studenti durante le attività scolastiche, potranno essere utilizzati esclusivamente per fini didattici o per documentare e divulgare le attività della scuola (sito web , facebook della scuola). L'autorizzazione non consente l'uso dell'immagine in contesti che pregiudichino la dignità personale ed il decoro della persona e per uso e/o fini diversi da quelli sopra indicati. In caso di partecipazioni a concorsi o manifestazioni l'Istituto specifiche, potrà essere richiesta ai genitori degli alunni apposite ulteriore autorizzazione che si procederà ad acquisire tramite la modulistica fornita dalla scuola stessa. La formula utilizzata per chiedere il consenso è sempre comprensibile, semplice e chiara. Pertanto, in ottemperanza al GDPR (General Data Protection Regulation) e al D. Lgs. 10 agosto 2018, n. 101, la scuola non si impegna solo a tutelare la privacy degli/lle studenti/esse e delle loro famiglie, ma anche ad informare e soprattutto rendere consapevoli gli/le studenti/esse e le loro famiglie di quanto sia importante tutelare il diritto alla riservatezza proprio e altrui.

3.2 - Accesso ad Internet

Si premette quanto segue:

- L'accesso a Internet oggi è un diritto fondamentale della persona, nonché condizione per il suo pieno sviluppo individuale e sociale.
- Ogni persona ha diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate; a tal fine va rimosso ogni ostacolo di ordine economico e sociale.
- Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.
- L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni..
- 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.

Tutto quanto sopra riportato è previsto dall'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Precedentemente, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e ancor prima quello del Consiglio del 25 novembre 2015, che avevano già individuato dettagliatamente le "misure riguardanti l'accesso a un'Internet aperto, modificando 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 da tempo presente nell'ordinamento italiano ed europeo, pertanto 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 contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, e le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa e matura.

L'accesso a Internet per la didattica è oggi una realtà presente in tutti i plessi del comprensivo, attraverso reti WiFi. La Dirigenza e l'Amministrazione dispongono invece di una rete separata che non grava su quelle dedicate alla didattica. Le LIM e i computer presenti nei laboratori e nelle aule sono manutenuti dalla ditta contrattualizzata responsabile dei laboratori, la quale segnala alla segreteria eventuali malfunzionamenti e disservizi ed installa un filtro di protezione per la navigazione dei minori per consentire, in sicurezza, l'accesso ad Internet. Tale accesso a scuola da parte degli studenti, avviene solo in presenza dell'insegnante, che è responsabile del loro comportamento, dell'uso delle macchine e dei software che vengono impiegati. Per ragioni di sicurezza, è possibile effettuare nuove installazioni e aggiornamenti di software solo tramite la password di amministratore, fornita esclusivamente al personale di assistenza tecnica. Anche l'accesso al sistema informatico per la didattica è consentito al personale tramite password. L'accesso ai portali istituzionali come SIDI, Istanze on-line, Segreteria Digitale, piattaforma PON ecc. prevede sempre l'uso di credenziali personali, mentre l'accesso a portali tematici si effettua per mezzo di password uniche condivise tra i referenti dei progetti e la dirigenza. I docenti possono accedere alla propria sezione del Registro elettronico con credenziali personali. Anche i genitori degli alunni sono provvisti di credenziali personali per la consultazione del Registro elettronico relativamente al profilo scolastico del proprio figlio. I computer d'uso quotidiano presenti nelle aule per le attività didattiche, non richiedono invece una password di accesso per l'accensione. Tutti i docenti dell'Istituto e gli studenti possiedono un account generato dalla scuola per consentire loro l'accesso a piattaforme didattiche utilizzate per la DAD.

È severamente vietato appropriarsi di password altrui ed usarle .

La scuola (Amministrazione e Dirigenza) utilizzano l'indirizzo di posta istituzionale per le comunicazioni, assieme al sito web della scuola.

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 agile e collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

Il sito dell'Istituto Comprensivo, sempre aggiornato, è un importante strumento comunicativo; esso è consultabile all'indirizzo: www.icleopardi.edu.it. La sua gestione e la rispondenza alle normative per quanto concerne i contenuti (accuratezza, appropriatezza, aggiornamento) e le tecniche di realizzazione e progettazione sono a cura del Dirigente Scolastico e dell'Animatore Digitale. L'inserimento dei dati, previa autorizzazione del DS, è ad opera dell'Animatore Digitale, del DSGA e dell'Assistente Amministrativa Maria Teresa Commone. Sul sito è possibile trovare il Regolamento d'Istituto, la

pubblicizzazione di eventi, gli avvisi per l'utenza, la documentazione di attività curricolari ed extracurricolari svolte. Pulsanti attivi permettono l'accesso a link di interesse, tra cui il registro elettronico. Alle aree riservate dove sono caricate comunicazioni interne specifiche, possono accedere tramite password personale solo le persone a cui l'aria è riservata.

La scuola, in qualità di ente pubblico, ha cura di pubblicare sul proprio sito web solo i contenuti che saranno valutati come pertinenti alle finalità educative istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative.

Dallo scorso anno l'istituzione scolastica ha adottato la versione AGID del sito scolastico.

La scuola si è dotata di un Regolamento sull'utilizzo dei social network, di Classroom e per le applicazioni di messaggistica.

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 la didattica e gli stili di apprendimento. Comprendere il loro corretto utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche del progetto Generazioni Connesse e del più ampio PNSD.

Il presente documento di e-Policy contiene indicazioni, revisioni ed 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 stabiliti dal 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, sia quelli positivi che le eventuali criticità afferenti il settore della didattica.

Come da Regolamento d'Istituto agli studenti è fatto assoluto divieto di usare all'interno dell'Istituto scolastico, se non per scopi esclusivamente didattici autorizzati dal docente, smartphone e/o ogni altro apparato multimediale (walkman, mp3, ipod, ipad, notebook, fotocamera, videocamera, ecc...).
Il divieto non si applica soltanto all'orario delle lezioni, ma all'intera permanenza dell'alunno all'interno della struttura scolastica (intervalli, pausa mensa...). I predetti dispositivi devono essere spenti ed opportunamente custoditi in borsoni, zaini, giacconi, mai collocati sul banco o tra le mani.
Come da Regolamento d'Istituto, ai sensi della C.M. n.362 del 25/08/98, i docenti non possono utilizzare i telefoni cellulari durante l'orario di lavoro. E' consentito l'uso di dispositivi elettronici personali solo a scopo didattico ed integrativo rispetto a quelli scolastici disponibili.

Per il personale ATA della scuola è vietato l'utilizzo di dispositivi elettronici durante l'orario di servizio, se non autorizzati.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022.

- Organizzare incontri formativi sull'uso sicuro delle tecnologie digitali (cybersecurity), rivolti al personale scolastico ed agli alunni.

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

- Promuovere costantemente eventi ed incontri formativi sull'uso sicuro delle tecnologie digitali (cybersecurity), rivolti al personale scolastico ed agli alunni.

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 gli altri;
- diventare una vittima di queste azioni;
- osservare altri commettere queste azioni e quindi essere spinto all'emulazione.

È importante prendere coscienza di questi possibili rischi e saperli distinguere, in modo da poter poi adottare le strategie migliori per arginarli. E' fondamentale operare in tal senso, preventivamente per ridurre la possibilità che questi fenomeni pericolosi avvengano, e ciò accade lavorando instancabilmente e sinergicamente su aspetti di ampio raggio che possano permettere una riduzione dei fattori di rischio e, quindi, una minore probabilità che i minori vengano a trovarsi in situazioni critiche. È importante, all'uopo, che i minori abbiano gli strumenti idonei per riconoscere le possibili situazioni di rischio e gli inganni della rete e che li segnalino immediatamente 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 mettere in campo 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 saper illustrare le possibili soluzioni e i comportamenti da adottare.

La prevenzione comprende, invece, un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere l'acquisizione delle competenze digitali da parte dei minori, affinché, attraverso un uso consapevole della rete e dei devices, imparino ad evitarne i rischi possibili.

La necessità di sensibilizzare gli studenti ad un utilizzo sicuro e consapevole delle tecnologie digitali, sia in un'ottica di tutela dai rischi potenziali che di valorizzazione delle opportunità esistenti, pone tutta la comunità educante di fronte alla sfida di riconsiderare concretamente la propria identità, le proprie risorse e il proprio ruolo educativo.

L'Istituto Comprensivo Giacomo Leopardi intende perseguire azioni di prevenzione universale e di sensibilizzazione, attraverso un'efficace integrazione con la rete dei servizi territoriali locali (Polizia postale, ASL,Associazioni non profit...), al fine di formare e consolidare quelle competenze educative di base necessarie a poter gestire le situazioni di vita che i ragazzi sperimentano online.

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, tratta ampiamente questo fenomeno, definendolo in questi termini:

"… è 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, realizzato 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 ed azioni utili a prevenire e a gestire i casi di cyberbullismo. Le Linee prevedono azioni preventive, educative e, in questo spirito formativo anche misure sanzionatorie che qui di seguito sintetizziamo in punti programmatici:

- la formazione del personale scolastico e la nomina di un proprio referente per ogni autonomia scolastica;
- l'implementazione e lo sviluppo delle competenze digitali;
- la promozione di un ruolo attivo degli studenti in attività di peer education;
- la previsione di misure di sostegno e rieducazione dei minori coinvolti;
- l'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 bullismo è, come il cyberbullismo (che rappresenta la sua più recente versione digitale), è un fenomeno assolutamente negativo e va contrastato e prevenuto fortemente, specie in ambio scolastico. Con questo termine di origine inglese, si definiscono tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e vessare, fisicamente e/o psicologicamente, un soggetto debole (o a volte un piccolo gruppo).

Il cyberbullismo presenta le seguenti caratteristiche:

- è invasivo: il bullo può raggiungere la sua vittima in qualsiasi momento e in qualunque luogo;
- è un fenomeno persistente: il materiale messo online vi può rimanere per molto tempo o per sempre se non rimosso;
- ha una platea potenzialmente infinita: le persone che possono subire o assistere agli atti di cyberbullismo sono potenzialmente illimitate.

A seconda dei casi, si potranno adottare tre tipologie di azioni : prevenzione universale, prevenzione selettiva e prevenzione indicate. Le riportiamo di seguito:

1. **Prevenzione Universale**. Un programma di questo tipo parte dal presupposto che tutti gli studenti siano potenzialmente a rischio. Si tratta quindi di interventi diretti al grande pubblico o ad un intero gruppo di una popolazione. Efficacia: trattandosi di programmi ad ampio raggio gli effetti di questi programmi possono essere modesti se confrontati con programmi che "trattano" un piccolo gruppo con un problema specifico. Tuttavia, questi interventi possono produrre cambiamenti a grande raggio e rivolgersi a grandi numeri (ad es. si pensi ad un programma dedicato alle competenze emotive, oppure alla cittadinanza digitale).

2. **Prevenzione Selettiva**. Un programma dedicato ad un gruppo di studenti in cui è presente il rischio online. In questo caso la presenza del rischio è stata individuata tramite precedenti indagini, segnalazioni fatte dalla scuola, oppure dalla conoscenza di fattori di rischio in quel determinato territorio. In questi casi gli interventi sono mirati e prevedono programmi formativi strutturati che hanno l'obiettivo di migliorare le competenze digitali e le strategie di problem solving. Efficacia: può essere un valido programma se si osservano casi in cui la prevenzione universale non ha dato gli esiti previsti.

3. **Prevenzione Indicata**. E' un programma di intervento rivolto al caso specifico, e quindi pensato e strutturato per adattarsi ad un gruppo preciso di studenti/studentesse con l'obiettivo di ridurre i comportamenti problematici, oppure dare supporto alle vittime. Efficacia: per la sua natura questo tipo di intervento si avvale di professionalità diverse (anche psicologi), in quanto perché affronta problemi legati alla salute mentale del minore. In questo intervento è opportuno coinvolgere anche la stessa famiglia del minore.

Il Referente per il bullismo ed il cyberbullismo, nominato in ogni istituzione scolastica, è un docente particolarmente sensibile a queste tematiche ed ha il compito di coordinare, in sinergia con il Dirigente scolastico, le iniziative di prevenzione e contrasto al bullismo ed al cyberbullismo deliberate nel PTOF, facendosi altresì promotore di buone pratiche presso i colleghi e gli studenti.

Si ricorda, infine, che nell'Istituto comprensivo è attivo uno Sportello Ascolto, attraverso il quale tutto il personale scolastico e l'utenza può avvalersi della consulenza gratuita di un esperto psicologo, selezionato con apposite bando e contrattualizzato dalla scuola, previa prenotazione. I minori possono usufruire del servizio solo con autorizzazione scritta dei genitori, da presentare al Dirigente scolastico.

4.3 - I PERICOLI IN RETE: l'Hate speech

L' *Hate speech* è un fenomeno di "incitamento all'odio" o "discorso d'odio", che si serve di discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che manifestano soprattutto in rete, 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 combattere gli stereotipi su cui spesso si fondano forme di *hate speech*, in particolare quelli legati alla razza, al genere, al credo religioso, all'orientamento sessuale, alla disabilità;

promuovere l'educazione civica, il rispetto reciproco e la collaborazione anche attraverso i media digitali e i social network;

favorire un uso della parola consapevole e costruttivo.

Lo sviluppo delle competenze digitali e l'educazione ad un uso eticamente corretto e consapevole delle tecnologie, assumono quindi un ruolo centrale anche per il contrasto di queste dinamiche in rete.
Occorre, in tal senso, valorizzare la dimensione relazionale del minore e fornire ai più giovani gli strumenti necessari per destrutturare gli stereotipi su cui spesso si fondano tali forme di hate speech.

L'Istituto, in tale attività formative, si avvarrà anche di consulenti/esperti esterni per organizzare incontri formativi rivolti a docenti, genitori ed alunni (Carabinieri, Polizia Postale, equipe Formazione Territoriale del MIUR, associazioni del Territorio preposte allo scopo, Magistrati e giuristi del Tribunale di Torre Annunziata, genitori esperti, ecc.);

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 e forme di dipendenza, può causare isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e ossessiva voglia di utilizzo della Rete (Next addiction).

Tale dipendenza, che può manifestarsi nel minore anche attraverso le tante ore trascorse nei giochi online o sui social, rappresenta una questione importante per la comunità scolastica, che deve attenzionare il fenomeno e fornire agli studenti e alle studentesse gli strumenti per combattere l'iperconnessione.

L'Istituto si propone di promuovere un uso maggiormente consapevole delle tecnologie, per favorire il "ben essere digitale", ossia la capacità di creare e mantenere una relazione sana con la tecnologia.
Gli elementi che contribuiscono al ben essere digitale sono:

- la ricerca di equilibrio anche nelle relazioni online, l'uso degli strumenti digitali per il raggiungimento di obiettivi personali;
- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile;
- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche);
- la capacità di controllare I tempi di connessione e di pianificarli in modo equilibrato, non sottraendo, tra l'altro, ore preziose allo studio, allo sport e al sonno.

Se controlliamo la tecnologia possiamo usare il pieno potenziale che essa offre e trarne grossi vantaggi!

È importante, quindi, non demonizzare apriori la tecnologia, ma cercare di saper entrare nel modo giusto, nel mondo degli studenti e delle studentesse, aiutando i nostri spesso inconsapevoli "native digitali" a maturare un'adeguata consapevolezza del loro approccio con le TIC, così che il "navigare" nel rispetto di poche e chiare regole condivise, non diventi all'insegna di un irresponsabile e pericolosa anarchia, quel triste "naufragio" di cui purtroppo tante volte ci parlano le cronache. A tale scopo sarà fondamentale concordare una linea condivisa con le famiglie dei minori, per stabilire insieme tempi,

mezzi e modalità da attuare durante lo studio domestico e forme di controllo attivo durante la navigazione in Rete.

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 emotivamente impattanti per i protagonisti delle immagini, delle foto e dei video. Spesso tali immagini o video, anche se inviate ad una stretta cerchia di persone, si diffondono in modo incontrollabile, perchè facilmente scaricabili, condivisibili e modificabili, e possono creare seri problemi, sia personali che legali, alla persona ritratta. L'invio di foto che riguardano minorenni in pose sessualmente esplicite configura, infatti, il reato di distribuzione di materiale pedopornografico.

I contenuti sessualmente espliciti possono, inoltre, diventare materiale di ricatto, assumendo la forma di "*revenge porn*" ossia "vendetta porno"; un fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte.

I rischi del sexting, legati al *revenge porn*, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotive con conseguenze inevitabili anche sul corpo, ansia diffusa, sfiducia nell'altro/i e depressione. Si contano, purtroppo, anche non pochi casi di suicidi.

4.6 - Adescamento online

Il *grooming* (dall'inglese "*groom*": curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti abusanti potenziali 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).

La problematica dell'adescamento online (come quella del sexting) si inquadra in uno scenario più ampio di immaturità, insicurezza, scarsa educazione emotivo/sessuale e assenza di competenza digitale. Al fine di prevenire casi di adescamento online è opportuno, pertanto, accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività, per renderli emotivamente più sicuri e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante il coinvolgimento dei genitori che devono attenzionare i propri figli e vigilare sull'uso che essi fanno dei canali digitali social. È importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma piuttosto soccorso, compreso ed ascoltato.

Fondamentale quindi, è portare avanti un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine, dell'identità online e delle relazioni online, con la consapevolezza che la peculiarità del mezzo/schermo permette a chiunque di potersi presentare molto diversamente da come realmente è.

Se si sospetta o si ha la certezza di un caso di adescamento online, è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere all'adescatore e che il computer o

altri dispositivi elettronici del minore -vittima, non vengano usati così da eliminare o compromettere le eventuali prove. I casi di adescamento online richiedono l'intervento della Polizia Postale a cui bisogna rivolgersi il prima possibile; vanno conservate le tracce degli scambi fra il minore e l'adescatore, salvate le conversazioni attraverso screenshot, memorizzando eventuali immagini o video, ecc. L'adescamento è una problematica molto delicata da gestire e può avere significative ripercussioni psicologiche sul minore.

È importante rivolgersi, inoltre, successivamente, ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, Sportello Ascolto della scuola, psicologo ecc..) in grado di fornire alla vittima quell' adeguato supporto di tipo psicologico necessario a curare le sue eventuali ferrite interiori.

4.7 - Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.); essa 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, concreti o simulati 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 ed, 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. La legge ha introdotto, 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,è realizzato con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, ma la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Secondo la Legge 172/2012 - Ratifica della Convenzione di Lanzarote (Art 4.), con il termine 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". Nell'ottica preventiva, il tema della pedopornografia è estremamente delicate ed occorre parlarne sempre con delicatezza, in considerazione della fascia d'età del minore, selezionando con cura il tipo di informazioni che si possono condividere. 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 e incontri con esperti sul tema.

Va all'uopo precisato che, qualora navigando in Rete si incontri materiale pedopornografico, è opportuno segnalarlo, anche anonimamente, all'indirizzo: 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 ad 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 pedopornografico e illegale 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 primariamente, ad identificare i minori presenti nelle immagini e video, assicurando la fine di un abuso che potrebbe essere ancora in corso.

Parallelamente, per salvaguardare il benessere psicofisico degli alunni coinvolti nella visione di questi contenuti, sarà opportuno ricorrere a un supporto psicologico anche passando per una consultazione del 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 si deve denunciare il fatto alle Forze dell'Ordine: 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.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022.

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

Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento della Polizia Postale;

Attivazione "Sportello Ascolto"

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

Organizzare incontri periodici di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse;

. Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse (Fondazione Carolina) + (Bullistop: Associazione nazionale, Enti e Associazioni non profit, selezionati dalla scuola);

Organizzare uno o più eventi e/o dibattiti in momenti extra- scolastici, sui temi della diversità e sull'inclusione rivolti a genitori;

Attivazione "Sportello Ascolto"

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 a cui attenersi. Questa sezione dell'e-Policy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse . Tali procedure dovranno essere una guida costante per il personale scolastico nell'identificazione di una situazione online a rischio, per la presa in carico da parte della scuola della situazione critica e per la definizione dell'intervento da mettere in atto per aiutare studenti/esse in difficoltà. 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 agli studenti, alle studentesse, alle famiglie e a tutti coloro che vivono la scuola che essa è un luogo sicuro, attento al benessere di chi la frequenta, e quindi 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, durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

Problematiche e procedure:

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).I docenti del Consiglio di classe o il personale ATA che ne viene a conoscenza, devono avvisare il Dirigente scolastico, per iscritto e valutare con lui come procedure.

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. La situazione va segnalata al Dirigente scolastico, per iscritto, e costui provvederà a convocare le famiglie dei minori e a denunciare la situazione alle Forze dell'ordine, nonché a concordare con famiglie e docenti una strategia di intervento educativo volto al recupero del "ben essere " del minore. Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultra quattordicenne (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.

Per le segnalazioni 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

Può succedere, altresì, che i minori potrebbero riferire all'insegnante fatti o eventi personali o altrui, accaduti anche al di fuori della scuola, tali da mettere in allarme il docente. Sono da considerare degni di segnalazione:

- contenuti afferenti la violazione della privacy (foto personali, l'indirizzo di casa o il telefono,
- informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, ecc.);

- contenuti espressione di aggressività o violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);
- contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

I docenti devono avvisare per iscritto il Dirigente scolastico, che concorderà con loro il da farsi, convocando altresì le famiglie dei minori.

5.2. – I Docenti e le segnalazioni

L'insegnante, come si sa, riveste la qualifica di pubblico ufficiale; l'esercizio delle sue funzioni non è circoscritto al solo ambito dell'apprendimento, ossia alle attività strettamente didattiche (preparazione e tenuta delle lezioni, attività di verifica e valutazione dei contenuti appresi dagli studenti), ma si estende a tutte le altre azioni educative. Egli, dunque, vigila sulla sicurezza ed il "ben essere" dei minori che frequentano la scuola ed ha il compito di accompagnarli pedagogicamente, di ascoltarli, osservarli e guidarli nel percorso di crescita culturale, civico ed umano. Nell'esercizio delle sue funzioni potrebbe trovarsi a vivere una di queste situazioni:

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.

Nel primo caso il docente allerterà i suoi colleghi del Consiglio di classe, invitandoli a monitore con attenzione la situazione per il tempo necessario a fugare o confermare i sospetti. In caso di conferma, il consiglio di classe è tenuto a farne segnalazione scritta e sottoscritta al Dirigente che concorderà con i suddetti docenti il da farsi.

Nel secondo caso il docente è tenuto a fare immediata segnalazione scritta al Dirigente che convocherà il Consiglio di classe e concorderà con esso il da farsi.

Nessuno che venga a conoscenza di situazioni critiche che coinvolgono i minori può sottrarsi alle sue responsabilità o omettere il suo dovere di pubblico ufficiale ed educatore.

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 o persone a cui rivolgersi quali:

- 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 il bullismo e cyberbullismo;
- un docente della classe;
- Dirigente scolastico

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

Il Dirigente scolastico, ricevute le segnalazioni pervenute attraverso I vari canali monitorati dal docente referente o dalle persone coinvolte, valuterà caso a caso il da farsi, se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale, i Servizi Sociali o se il caso vada gestito all'interno della scuola con il coinvolgimento del Consiglio di Classe e delle famiglie degli alunni.

5.3. - Gli attori sul territorio

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

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

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

Comitato Regionale Unicef: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
Co.Re.Com. (Comitato Regionale per le Comunicazioni): svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.

Ufficio Scolastico Regionale: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
Polizia Postale e delle Comunicazioni: accoglie tutte le segnalazioni relative

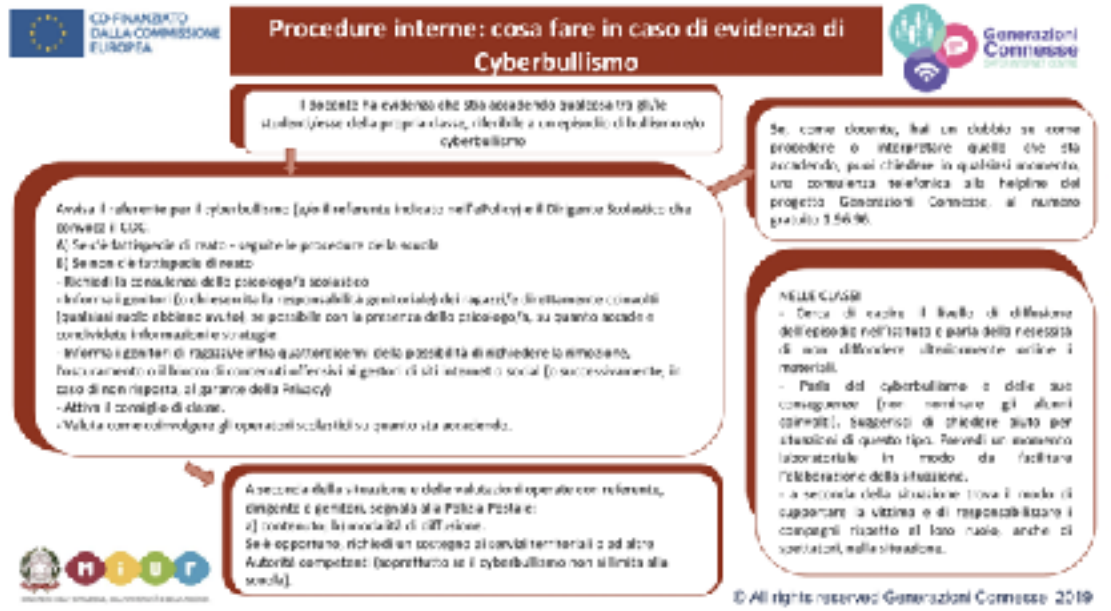
a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
Aziende Sanitarie Locali: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.

Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
Tribunale per i Minorenni: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

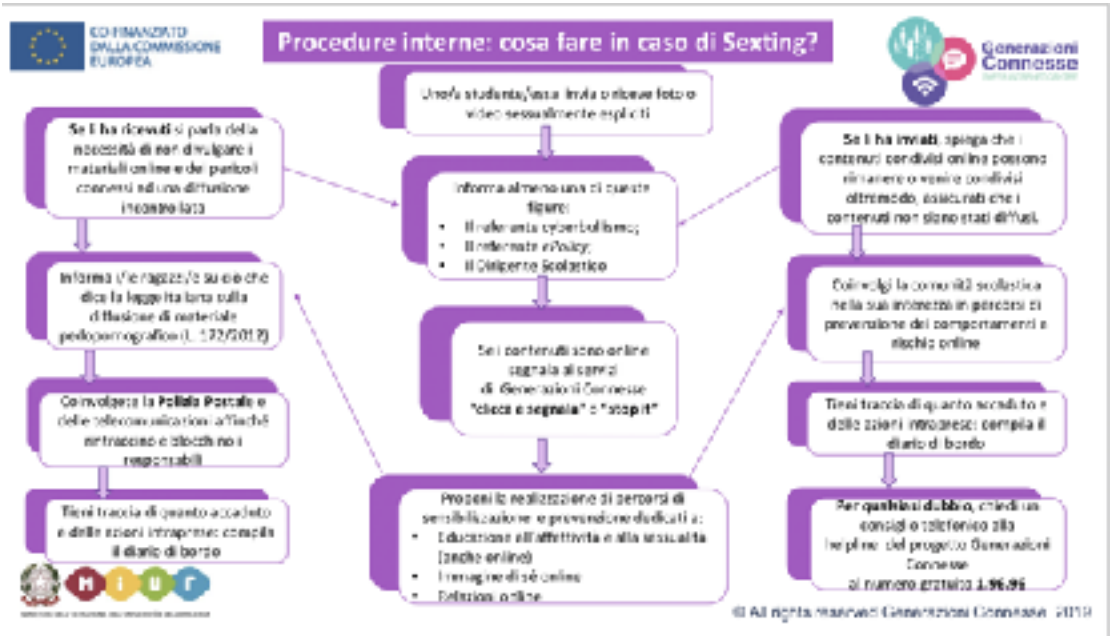
Nei casi di gravità, si procederà alla denuncia alle Forze dell'ordine e ai Servizi sociali.

5.4. - Allegati con le procedure

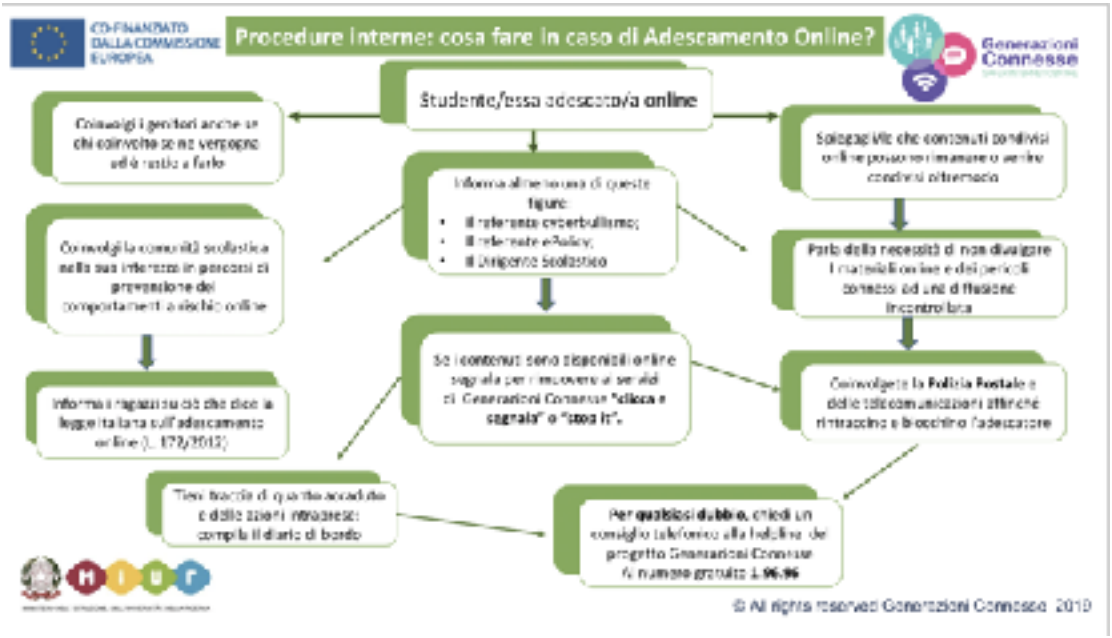
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



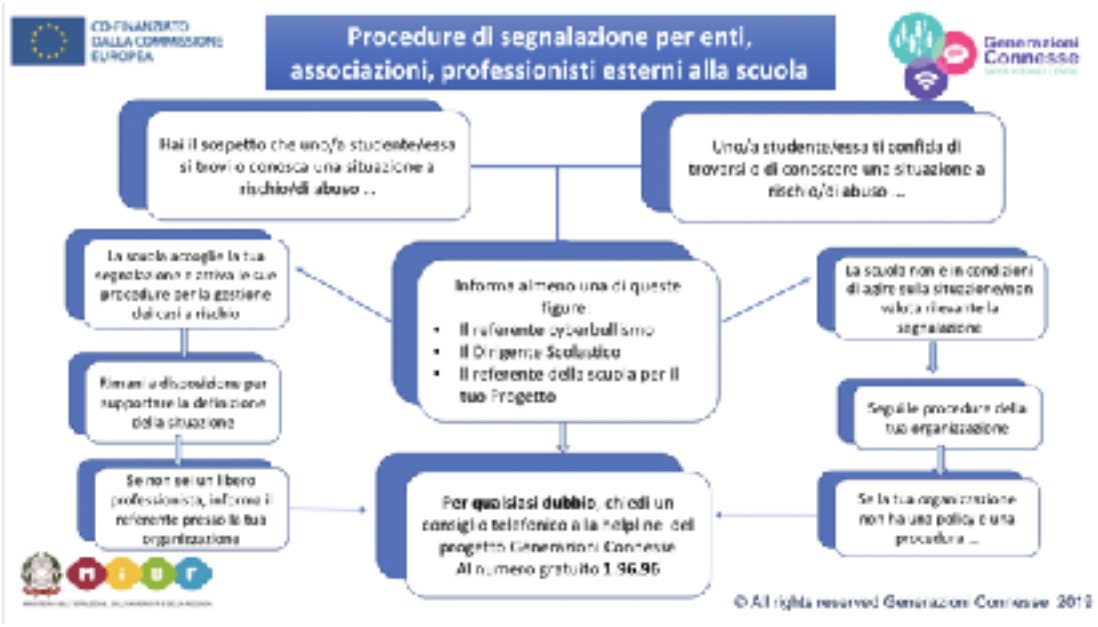
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?

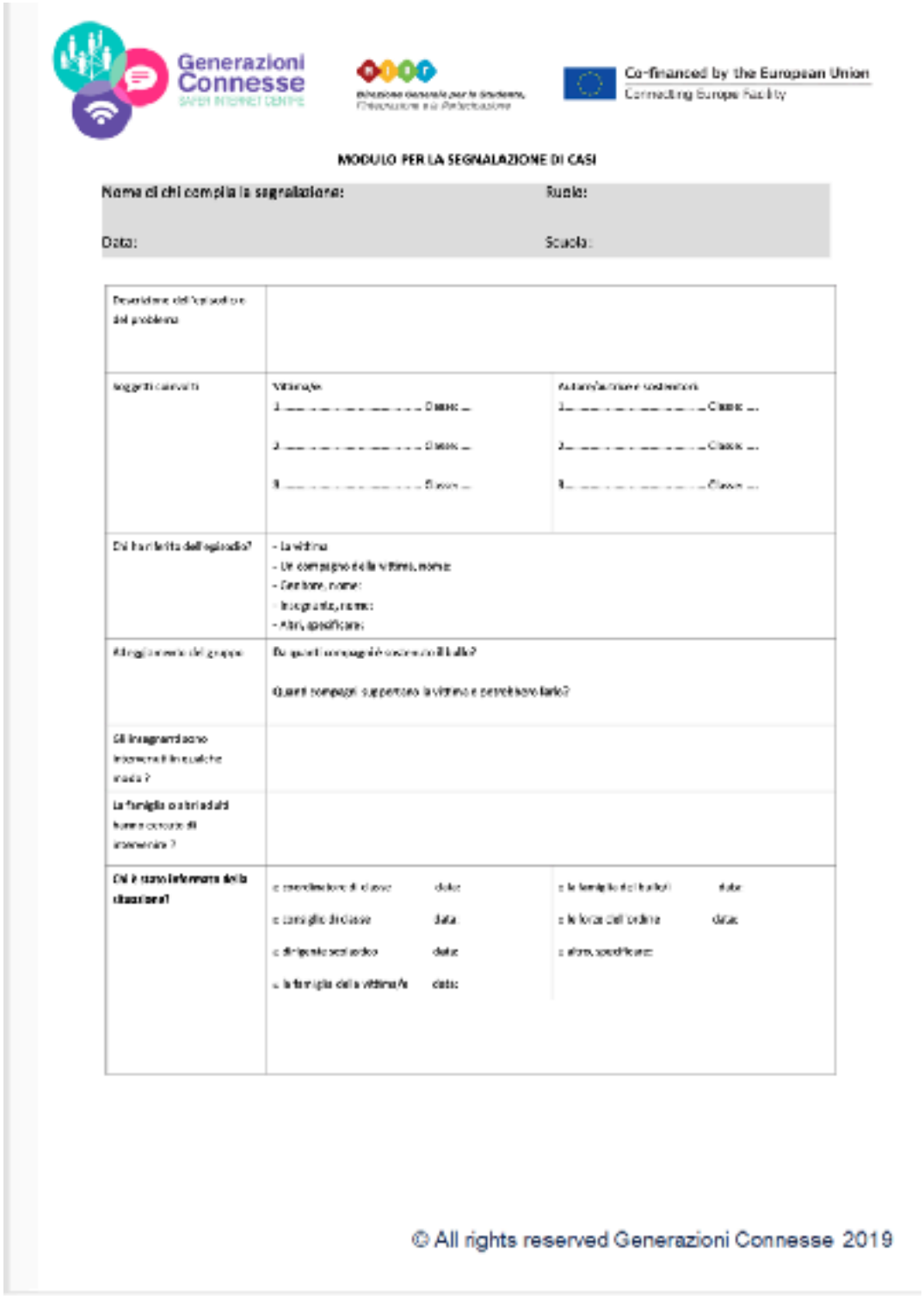


Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola



Altri allegati

Scheda di segnalazione



Generazioni Connesse
SAFER INTERNET CENTRE

Co-financed by the European Union
Connecting Europe Facility

MODULO PER LA SEGNALAZIONE DI CASI

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

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

Generazioni Connesse
SAFER INTERNET CENTRE

Co-financed by the European Union
Connecting Europe Facility

MODULO PER IL FOLLOW-UP DEI CASI

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

Diario di bordo

CO-FINANZIATO DALLA COMMISSIONE EUROPEA

Sicurezza in rete - Schema per la scuola

Generazioni Connesse

Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi
Scuola _____ Anno Scolastico _____

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

iGloss@ 1.0 l'ABC dei comportamenti devianti online Elenco reati procedibili d'ufficio

L'allegato è disponibile sul sito web della scuola.

Procedure operative per la gestione delle infrazioni alla E-Safety Policy

Ogni volta che un membro del personale o studente viola la E-Safety Policy, la decisione finale sul livello di sanzioni sarà disposta dal Dirigente Scolastico nel rispetto delle procedure comportamentali e disciplinari della scuola.
Si rimanda pertanto al Regolamento d'Istituto vigente.

Progetto regionale:
"Responsabili in classe e on-line"
www.responsabilionline-fvg.it

ISTITUTO COMPRENSIVO GEMONA DEL FRIULI

media educazione comunità

Scheda di approfondimento: I PRINCIPALI REATI PROCEDIBILI D'UFFICIO

Gli insegnanti, in quanto incaricati di pubblico servizio, hanno obbligo di denuncia qualora vengano a conoscenza di reati perseguibili d'ufficio. A questa categoria appartengono i seguenti reati:

Delitti "sessuali" (art. 609 bis e seguenti c.p.)
a) Violenza sessuale commessa nei confronti di minore di anni 18;
b) Violenza commessa dal genitore (anche adottivo) o dal di lui convivente, dal tutore o da persona alla quale il minore sia affidato per ragioni di cura, di educazione, di istruzione, di vigilanza o di custodia;
c) Violenza sessuale di gruppo;
d) Corruzione di minorenne (chi compie atti sessuali in presenza di un minore di 14 anni al fine di farlo assistere; chi fa assistere l'infra-quattordicenne ad atti sessuali o mostra materiale pornografico al fine di indurlo a compiere o subire atti sessuali);
e) Adescamento di minorenni (chi allo scopo di commettere reati di prostituzione minorile, pornografia minorile, detenzione di materiale pornografico, violenza sessuale, ...adesca un minore infra-sedicenne).

Prostituzione minorile* (600 bis)
Punisce chi recluta o induce alla prostituzione un minore di 18; favorisce, sfrutta, gestisce, ...la prostituzione di un minore di 18 anni; chi compie atti sessuali con un minore tra i 14 e i 18 anni in cambio di corrispettivo di denaro o altra utilità, anche solo promessi.

Pornografia minorile* (art. 600 ter) e Detenzione di materiale pedopornografico* (art. 600 quater c.p.)
Il presenti reati puniscono: chi utilizzando minori di anni diciotto realizza esibizioni o spettacoli pornografici ovvero produce materiale pornografico; chi recluta, induce minori di anni diciotto a partecipare a tali esibizioni o ne trae profitto; chi anche con il mezzo telematico, distribuisce, divulga, pubblicizza notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori di 18 anni; chi assiste a esibizioni o spettacoli pornografici in cui sono coinvolti minori di 18 anni; chi consapevolmente si procura, detiene, offre o cede ad altri, anche a titolo gratuito il materiale pornografico realizzato utilizzando minori di anni diciotto.

Minaccia* (art. 612 c.p)
Se qualcuno viene minacciato in modo grave (p.e. di morte) o con armi.

Lesione personale* (art. 582 c.p.)
Punisce chi procura lesione da cui deriva una malattia nel corpo o nella mente con prognosi superiore a 20 giorni o con circostanze aggravanti.

Stalking - atti persecutori* (art 612 –bis)
Chiunque, con condotte reiterate, minaccia o molesta un minore o una persona con disabilità (art.3 della legge 104/92) in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva, ovvero da costringere lo stesso ad alterare le proprie abitudini di vita.

Istigazione al suicidio* (art. 580 c.p.)
Chiunque determina altri al suicidio o rafforza l'altrui proposito di suicidio, ovvero ne agevola in qualsiasi modo l'esecuzione, è punito, se il suicidio avviene, con la reclusione da cinque a dodici anni. Se il suicidio non avviene, è punito con la reclusione da uno a cinque anni, sempre che dal tentativo di suicidio derivi una lesione personale grave o gravissima.

Estorsione* (art. 629 c.p.)
Punisce chi mediante violenza o minaccia costringe una persona a fare o omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno.

Violenza privata* (art. 610 c.p.)
Se una persona viene costretta con violenza o minaccia a fare, tollerare o omettere qualcosa (ad es. dover andare con qualcuno, ovvero non poter uscire ecc).

Sostituzione di persona* (art. 494 c.p.)
Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici.

Delitti contro l'assistenza famigliare (artt. 570 e seg. c.p.)
a) Violazione degli obblighi di assistenza famigliare se commessi nei confronti di minori
b) Abuso di mezzi di correzione o di disciplina;
c) Maltrattamenti in famiglia o verso i fanciulli.

***REATI ON-LINE:** la maggior parte dei reati sopra citati **possono essere commessi anche on-line** ovvero attraverso l'utilizzo di dispositivi connessi alla rete. Questa circostanza, che spesso rende più difficile l'individuazione del reato e più facile la sua attuazione da parte dei minori, può costituire in alcuni casi una aggravante del reato stesso.
Non ci sono tuttavia **reati specifici che descrivono questi comportamenti on-line e si deve quindi fare riferimento ai reati sopra elencati**. Ad esempio i comportamenti come il **Cyberbullismo** e il **Sexting** vanno valutati caso per caso in quanto possono includere uno o più dei reati perseguibili d'ufficio sopra elencati.

Informazioni in caso di necessità di un parere legale

-**Riferimento Nazionale: tel. 19696** - http://consulenzaonline.azzurro.it/xchatty/chat.html
(Telefono Azzurro – progetto Nazionale Generazioni Connesse)

-**Riferimento Regionale: tel. 0432.555708** Mail: garantefvg@regione.fvg.it
(Garante Regionale dei diritti alla persona del Friuli Venezia Giulia)