Documento di ePolicy

SIIC819006

FEDERIGO TOZZI - CHIANCIANO T.

VIALE DANTE N. 35 - 53042 - CHIANCIANO TERME - SIENA (SI)

MARCO MOSCONI

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse.

Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali. Nello specifico:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

Argomenti del Documento

Perché è importante dotarsi di una E-policy?

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi

all'uso di Internet.

L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

La diffusione delle nuove tecnologie nella vita quotidiana ha coinvolto anche il mondo della scuola ed ha imposto la necessità di verificare modalità di utilizzo e regolamentazione dei diversi strumenti e strutture. Le nuove dotazioni digitali condizionano e influenzano la didattica. Il loro utilizzo deve pertanto essere definito e regolamentato in un'ottica di tutela degli utenti, in particolare perché minori di età. L'Istituto Comprensivo "Federigo Tozzi " di Chianciano Terme, ritiene che l'utilizzo e l'educazione ad un uso consapevole delle tecnologie digitali rappresenti una sfida irrinunciabile in questo momento storico. Per raggiungere tale obiettivo, si avvale delle piattaforme cloud G Suite for Education e Edmodo.

Attraverso l'account di Istituto i docenti e gli studenti possono usufruire delle applicazioni messe a disposizione da entrambe le piattaforme che negli ultimi anni hanno sempre più integrato i loro strumenti. In particolare la G Suite ha assunto un ruolo centrale per quanto riguarda l'uso di mail, di creazione di documenti e loro condivisione.

Il presente documento di e-policy disciplina l'uso dei suddetti strumenti digitali a partire dall'anno scolastico 2020/2021. Tutti gli utenti sono tenuti a conoscere le regole relative all'uso dei servizi della Google Suite e anche ad informarsi sulle norme nazionali e internazionali che regolamentano l'uso delle piattaforme on line e che sono contenute nei seguenti decreti:

● Codice In Materia Di Protezione Dei Dati Personali - Decreto Legislativo 30 giugno 2003, n. 196;

● Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 e successive modifiche e integrazioni;

● Disposizioni legislative in materia di documentazione amministrativa. - Decreto 14 novembre 2007, n. 239, regolamento attuativo dell'articolo 71-bis della legge 22 aprile 1941, n. 633, in materia di diritto d'autore; ●Decreto Legislativo 10 Agosto 2018, n.101; ●Regolamento Ue 2016/679 e Decreto Legislativo 18 maggio 2018, n. 51 (attuazione della direttiva).

1. Definizioni

Nel presente documento i termini qui sotto elencati hanno il seguente significato:

Istituto: Istituto comprensivo "Federigo Tozzi" di Chianciano Terme-Amministratore di sistema: il responsabile incaricato dal Dirigente Scolastico per l'amministrazione del

servizio -Servizio: GSuite for Education, messo a disposizione della scuola (Animatore Digitale)

Fornitore: Google

Utente: colui che utilizza un account del servizio Account: insieme di funzionalità, applicativi, strumenti e contenuti attribuiti ad un nome utente con le credenziali di accesso.

2. Natura e finalità del servizio

Il servizio consiste nell'accesso agli strumenti della piattaforma "Google Suite for Education" ed è inteso come supporto alla didattica e ai servizi correlati con le attività scolastiche in generale: pertanto gli account creati devono essere utilizzati esclusivamente per tali fini. Per ora la struttura della mail/username è divisa fra docenti e studenti. Per i docenti è:
nome@comprensivochiancianoterme.it; per gli studenti è cognome@comprensivochiancianoterme.it. In caso di omonimia per i docenti :

è nomecognome@comprensivochiancianoterme.it;

per gli studenti cognomenome@comprensivochiancianoterme.it. L'istituto utilizza server Google per l'erogazione del servizio oggetto del presente documento, su tali server ogni utente avrà a disposizione:

a) CASELLA DI POSTA ELETTRONICA nel dominio comprensivochiancianoterme.it. La casella è strettamente personale e non è ammesso l'utilizzo da parte di persone diverse dall'assegnatario, né questi può cederla a terzi. L'utente, pertanto, accetta di essere riconosciuto quale autore dei messaggi inviati dal suo account e di essere il ricevente dei messaggi spediti al suo account.

E' bene inoltre ricordare che gli account studenti sono settati in modo che NON possano né ricevere né inviare mail al di fuori del dominio comprensivochiancianoterme.it

b) I SERVIZI AGGIUNTIVI DI G SUITE previsti dalla convenzione con l'Istituto, senza la necessità di procedere ad alcuna installazione per la loro funzionalità (cloud). Le applicazioni a disposizione dell'utente, fruibili via internet, sono attivabili o meno a discrezione dell'Istituto, che ne definisce di volta in volta regole e limiti di utilizzo, in base alle esigenze legate all'attività svolta, indipendentemente dalle possibilità tecniche offerte dalla piattaforma di Google. Il servizio è fornito gratuitamente ed è fruibile fino al termine del percorso di studio degli studenti o al termine dell'attività lavorativa del personale presso l'Istituto.

3. Soggetti che possono accedere al servizio

a) DOCENTI in servizio a tempo indeterminato e determinato, anche per supplenze brevi, i quali riceveranno le credenziali per l'accesso dall'Amministratore al momento

dell'assunzione e fino al termine dell'attività lavorativa presso l'Istituto.

b) STUDENTI, previa compilazione e consegna del modulo di autorizzazione firmato dai genitori se minorenni. Il servizio sarà fruibile fino al termine del percorso di studi presso l'Istituto

c) ALTRE CATEGORIE di utenti che possono richiedere la creazione di un account, sempre in relazione alle necessità didattiche e di comunicazione. Il servizio è limitato al dominio comprensivochiancianoterme.it, pertanto è condiviso dai soli membri interni all'organizzazione. Eventuali interazioni con l'esterno sono autorizzate dall'Amministratore in accordo con il titolare della licenza d'uso del servizio (il Dirigente Scolastico) e per specifiche esigenze organizzative e/o didattiche.

4. Dichiarazione

STUDENTI Ogni studente/studentessa riceverà la password per accedere ai servizi di G Suite e avrà accesso alla piattaforma solo dopo che gli stessi e i loro genitori (se minori) avranno accettato le regole di utilizzo, dichiarando inoltre di essere a conoscenza della normativa locale, nazionale ed europea vigente. DOCENTI E PERSONALE Il conferimento dei dati di cui alla presente informativa ha natura obbligatoria per quanto riguarda i dipendenti dell'Istituto in quanto previsto dall'art.47 del D.Lgs.82/2005 "Codice dell'Amministrazione Digitale" (e successive modificazioni). Pertanto non è necessario acquisire il consenso dell'interessato, ma solamente fornire la presente informativa (ex art.13 del D.Lgs.196/2003).

5. Durata del rapporto e cessazione del servizio STUDENTI L'uso dell'account per lo Studente ha durata quinquennale (dalla classe quarta della Scuola Primaria alla classe terza della Scuola Secondaria di I grado, salvo eccezioni motivate da scelte didattiche del personale docente) e viene rinnovato automaticamente all'atto dell'iscrizione all'anno successivo. Alla conclusione del percorso di studi o in caso di ritiro, dopo un mese, l'amministratore procederà alla disattivazione dell'account. Sarà quindi possibile recuperare i propri dati personali entro 30 giorni dalla cessazione del servizio. Successivamente l'indirizzo verrà eliminato.

DOCENTI E PERSONALE Per i docenti/personale ATA il servizio viene reso disponibile per tutto il periodo di permanenza presso l'Istituto e cessa con il termine del contratto, oppure in caso di trasferimento ad altro Istituto. Sarà possibile per il docente/personale recuperare i propri dati personali entro 3 mesi dalla cessazione del servizio. Successivamente l'indirizzo verrà eliminato. Nel caso di supplenze brevi, l'account sarà invece revocato dopo 15 giorni dal termine del contratto.

1.2 - Ruoli e responsabilità

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

L'imporsi delle nuove tecnologie nella vita personale, i rischi ad esse connesse, le potenzialità e l'esponenziale crescita dei contatti e delle relazioni pongono spesso il singolo di fronte alla realtà "concreta" e a quella virtuale, tra loro ormai fortemente connesse, influenzate e spesso determinate. La nascita, poi, di gruppi in rete richiede capacità comunicative e socio-relazionali adeguate. È fondamentale conoscere come comportarsi in questi gruppi, quali regole vanno rispettate e quali ruoli e responsabilità hanno i soggetti che vi partecipano. È opportuno che anche nell'ambito scolastico ci sia chiarezza sui ruoli e sulle responsabilità di ciascun attore del percorso formativo.

a. L'utente si impegna a non commettere violazioni della legislazione vigente, dei regolamenti dell'Istituto e di qualsiasi ulteriore regolamentazione stabilita dal responsabile o dall'amministratore. Si impegna altresì a rispettare le regole che disciplinano il comportamento nel rapportarsi con altri utenti e a non ledere i diritti e la dignità delle persone.

b. Ogni account è associato ad una persona fisica ed è strettamente personale. Le credenziali di accesso non possono, per nessun motivo, essere comunicate ad altre persone.

c. L'utente è responsabile delle azioni compiute tramite il suo account e, pertanto, esonera l'Istituto da ogni pretesa o azione che dovesse essere rivolta all'Istituto medesimo da qualunque soggetto, in conseguenza di un uso improprio.

d. Gli utenti prendono atto che è vietato servirsi o dar modo ad altri di servirsi del servizio di posta elettronica e delle applicazioni Google messe a disposizione dall'Istituto per danneggiare, violare o tentare di violare il segreto della corrispondenza e il diritto alla riservatezza.

e. Gli utenti si impegnano, inoltre, a non trasmettere o condividere informazioni che possano presentare forme o contenuti di carattere pornografico, osceno, blasfemo, diffamatorio o contrario all'ordine pubblico o alle leggi in materia civile, penale ed amministrativa vigenti.

f. Gli utenti, nel caso in cui utilizzino la strumentazione digitale dell'Istituto, hanno il dovere di disconnettersi dal proprio account, una volta terminata l'attività; questo per evitare spiacevoli occasioni di violazione della privacy. La password personale non va pertanto memorizzata sui dispositivi non personali.

7. Obblighi degli utenti Obblighi dello Studente

Lo Studente/La studentessa si impegna a:

- modificare immediatamente al primo ingresso la password provvisoria che gli/le sarà consegnata in modo che nessuno possa utilizzare impunemente la password altrui;
- conservare la password personale, non comunicarla e non consentirne l'uso ad altre persone (solo i genitori possono esserne custodi);
- assicurarsi di effettuare l'uscita dall'account e di rimuovere l'account dalla pagina web qualora utilizzi dispositivi non personali o ai quali potrebbero aver accesso altre persone;
- comunicare immediatamente attraverso e-mail all'amministratore l'impossibilità ad accedere al proprio account o il sospetto che altri possano avervi fatto accesso;
- non consentire ad altri, a nessun titolo, l'utilizzo della piattaforma G Suite;
- non diffondere eventuali informazioni riservate di cui venisse a conoscenza, relative all'attività delle altre persone che utilizzano il servizio;
- essere responsabile di quanto viene da lui/lei fatto nella chat e nella classe virtuale;
- non comunicare il codice di accesso alla classe a coloro che non ne fanno parte;
- accettare e rispettare le regole del comportamento all'interno della classe virtuale e le normative nazionali vigenti in materia di utilizzo di materiali in ambienti digitali;
- non pubblicare immagini, attività didattiche o extra-didattiche all'interno della classe virtuale senza previa autorizzazione dell'insegnante titolare della classe stessa. Lo studente/ssa e la sua famiglia si assumono la piena responsabilità di tutti i dati da loro inoltrati, creati e gestiti attraverso la piattaforma G Suite.
- leggere, comprendere e rispettare il documento di e-safety
- nell'utilizzo consapevole delle grandi possibilità di ricerca offerte dalla rete, rispettare le norme sul diritto d'autore, evitando il plagio
- adottare comportamenti rispettosi degli altri anche nella comunicazione in rete

8 Il docente e il personale si impegnano a:

● modificare immediatamente al primo ingresso la password provvisoria che gli/le sarà consegnata in modo che nessuno possa utilizzare impunemente la password altrui;

● conservare la password personale, non comunicarla e non consentirne l'uso ad altre persone;

● assicurarsi di effettuare l'uscita dall'account e di rimuovere l'account dalla pagina web qualora utilizzi dispositivi non personali o ai quali potrebbero aver accesso altre persone;

● comunicare immediatamente attraverso e-mail all'amministratore l'impossibilità ad accedere al proprio account o il sospetto che altri possano avervi fatto accesso;

● non utilizzare la stessa password per G Suite e Registro Elettronico;

● non consentire ad altri, a nessun titolo, l'utilizzo della piattaforma G Suite;

● non diffondere eventuali informazioni riservate di cui venisse a conoscenza, relative all'attività delle altre persone che utilizzano il servizio;

● essere responsabile di ogni proprio intervento nell'utilizzo delle applicazioni disponibili sulla piattaforma G Suite;

● attenersi alle regole incluse nella Netiquette.

●integrare le suddette tematiche nel curriculo scolastico

● assicurarsi che gli alunni rispettino la normativa sul copyright instaurare forme di comunicazione digitali con alunni e genitori improntate al codice di comportamento professionale, nell'ambito dei canali scolastici ufficiali

● garantire la riservatezza dei dati personali trattati ai sensi della normativa vigente

Obblighi del Dirigente scolastico

● È il soggetto su cui grava la responsabilità di garantire la sicurezza dei membri della comunità scolastica e, conseguentemente, anche la sicurezza in rete. In quest'ottica egli si preoccupa di:

● garantire a tutti i docenti ed alunni, soprattutto quelli in entrata, la formazione per l'uso responsabile e corretto delle Tecnologie dell'Informazione e della comunicazione (alcune ore di lezione all'anno sulla websecurity nelle TIC), sia per l'uso personale sia per la didattica;

● dotare la scuola di un sistema in grado di consentire il controllo della sicurezza in rete;

● seguire le procedure relative agli eventi dannosi eventualmente occorsi agli alunni nell'utilizzo delle TIC a scuola

● Obblighi dell'Animatore digitale;

● promuovere la formazione interna in ambito tecnologico-digitale •informare riguardo ai rischi della rete e coordinare, in collaborazione con il referente cyberbullismo, attività di sensibilizzazione e prevenzione in materia di bullismo e cyberbullismo2.

2 DSGA Il Direttore dei Servizi Amministrativi

● assicura, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici in grado di garantire un corretto funzionamento dell'infrastruttura tecnica dell'Istituto, sicura rispetto ad un uso scorretto e ad attacchi esterni

.Obblighi dei genitori

Anche i genitori sono coinvolti a pieno titolo. Ad essi è richiesto di

● sostenere i docenti nell'azione educativa mirata al corretto utilizzo delle tecnologie digitali;

● educare (vigilando sui propri figli) al corretto utilizzo delle tecnologie digitali in ambiente domestico fissando regole di comportamento e di utilizzo (eventualmente concordate con i docenti);

● collaborare con i docenti nell'adozione di linee di intervento coerenti per contrastare l'uso non responsabile, scorretto o pericoloso delle tecnologie digitali.

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

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

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

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

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

scolastica

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

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

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

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

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

Condividere e comunicare la politica di e-safety agli alunni -Tutti gli alunni saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione. - L'istruzione degli alunni riguardo all'uso responsabile e sicuro di internet precederà l'accesso alla rete;

● L'elenco delle regole per la sicurezza on-line sarà pubblicato in tutte le aule o laboratori con accesso a internet;

● Sarà data particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili".

2. Condividere e comunicare la politica di e-safety al personale

La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet sarà discussa negli organi collegiali e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web;

Per proteggere tutto il personale e gli alunni, la scuola metterà in atto una linea di condotta di utilizzo accettabile, controllato e limitato alle esigenze didattiche essenziali;

- Il personale docente sarà reso consapevole del fatto che il traffico in internet può essere monitorato e si potrà risalire al singolo utente registrato;

- Un'adeguata informazione/formazione on-line del personale docente nell'uso sicuro e responsabile di internet, sia professionalmente che personalmente, sarà fornita a tutto il personale, anche attraverso il sito web della scuola;

- Il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC sarà supervisionato dall'Animatore digitale, che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici;

1.5 - Gestione delle infrazioni alla ePolicy

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

Gestione delle infrazioni alla Policy. Per la natura stessa della comunicazione attraverso internet, non è possibile garantire che contenuti non idonei vengano visualizzati su un computer della scuola o su dispositivi mobili, non essendo possibile accertare responsabilità da parte della scuola o delle autorità preposte. Tuttavia gli utenti saranno informati sulle sanzioni in caso di infrazione della e-policy, sempre rapportate all'età e al livello di sviluppo degli alunni, oltre che alla gravità dell'infrazione stessa. Le eventuali infrazioni potranno riguardare: - un uso offensivo e lesivo della dignità propria e altui della comunicazione in rete comportamenti connessi al sexting - l'utilizzo delle tecnologie informatiche e dei dispositivi mobili non autorizzati dal docente - l'accesso a siti internet non autorizzati dal docente Le sanzioni includeranno:

-richiamo verbale

-richiamo scritto

- segnalazione al docente responsabile della sicurezza on line

---

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

UTILIZZO DEL LABORATORIO DI INFORMATICA, DELLE POSTAZIONI DI LAVORO E DELL' UTILIZZO DI INTERNET

Disposizioni sull'uso del laboratorio

1. Le apparecchiature presenti nella scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.

2. I laboratori informatici e le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.

3. Quando un insegnante, da solo o in classe, usufruisce del laboratorio deve obbligatoriamente registrare il proprio nome e l'eventuale classe nell'apposito registro delle presenze di laboratorio, indicando l'orario di ingresso, quello di uscita e motivazione dell'uso delle postazioni informatiche. Questo allo scopo di poter risalire alle cause di eventuali inconvenienti o danneggiamenti e per comprovare l'effettivo utilizzo dell'aula.

4. L'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante.

5. Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software.

6 Nei laboratori è vietato utilizzare CD personali o pen-drive se non dopo opportuno controllo con sistema di antivirus aggiornato.

7. E' vietato cancellare o alterare files-dati presenti sull'hard disk.

8. Il laboratorio non deve mai essere lasciato aperto o incustodito quando nessuno lo utilizza. All'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il mobilio in ordine, le macchine spente correttamente (chiudi sessione…)

9. In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile del laboratorio.

10. In caso di malfunzionamento non risolvibile dal responsabile di laboratorio si contatterà personalmente o attraverso il Responsabile di laboratorio, la segreteria.

11. Per motivi di manutenzione straordinaria, in caso di guasti o di virus, i PC possono essere formattati senza preavviso. Si consiglia pertanto di salvare i dati importanti su Cd o pen drive periodicamente. In caso di formattazione ordinaria ci sarà un preavviso.

Disposizioni sull'uso dei software

1. I software installati sono ad esclusivo uso didattico. 2. In base alle leggi che regolano la distribuzione delle licenze, i prodotti software presenti in laboratorio non sono disponibili per il prestito individuale. Nei casi in cui lo fossero in base a precise norme contrattuali i docenti interessati, dopo aver concordato il prestito con il Responsabile di laboratorio, devono compilare l'apposito registro di consegna software custodito in laboratorio.

3. E' fatto divieto di usare software non conforme alle leggi sul copyright. E' cura dell'insegnante utente di verificarne la conformità. Gli insegnanti possono installare nuovo software sui PC del laboratorio della propria scuola, previa autorizzazione scritta del DS solo se il software installato rispetta le leggi sul copyright.

4. E' responsabilità degli insegnanti che chiedono al Responsabile di laboratorio di effettuare copie di cd/dvd per uso didattico, di assicurarsi che la copia non infranga le leggi sul copyright in vigore.

Accesso a internet

1. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante;

2. Internet non può essere usato per scopi vietati dalla legislazione vigente;

3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet;

4. E' vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza. Norme finali Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica:

- Pubblicizzare il progetto e l'ePolicy.

Azioni da svolgere nei prossimi 3 anni:

- Organizzare 1 evento di presentazione e conoscenza dell'ePolicy rivolto agli studenti

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

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

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

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

"La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet". Il Curricolo della scuola del primo ciclo di istruzione sulle competenze digitali per gli alunni è trasversale alle discipline previste dalle Indicazioni Nazionali: la competenza digitale è ritenuta dall'Unione Europea competenza chiave, per la sua importanza e pervasività nel mondo d'oggi. L'approccio per discipline scelto dalle Indicazioni non consente di declinarla con le stesse modalità con cui si possono declinare le competenze chiave nelle quali trovano riferimento le discipline formalizzate. Si ritrovano abilità e conoscenze che fanno capo alla competenza digitale in tutte le discipline e tutte concorrono a costruirla.

Competenza digitale significa padroneggiare certamente le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con "autonomia e responsabilità" nel rispetto degli altri e sapendone prevenire ed evitare i pericoli. In questo senso, tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione.

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

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

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

L'Istituto ha aderito alle attività formative, promosse dal MIUR nell'ambito del PNSD, organizzate dagli snodi formativi e rivolte all'animatore digitale, al team per l'innovazione. Si prevede l'attivazione di iniziative di formazione facendo ricorso a soggetti esterni e/o al personale docente interno alla scuola che abbia acquisito competenze sull'innovazione didattica. Il percorso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica deve diventare un processo permanente che deve prevedere anche momenti di autoaggiornamento, di formazione personale o collettiva.

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

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno

organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc…), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

Coerentemente con quanto previsto dal PNSD, l'Istituto si avvale dell'Animatore Digitale, che coordina la diffusione dell'innovazione digitale e collabora con tutti i soggetti che possono contribuire alla realizzazione degli obiettivi del Piano. Anche il percorso della formazione specifica dei docenti sull'utilizzo consapevole e sicuro di INTERNET prevede momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi. Sono diffuse informazioni circa opportunità formative esterne in presenza e/o a distanza.l'IC "Tozzi" , inoltre, la promozione di attività formative interne (seminari, workshop, ecc), avvalendosi di risorse interne e/o esterne. Il docente referente partecipa a specifiche iniziative di formazione dedicate alla prevenzione e contrasto del bullismo e cyberbullismo

---

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

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

Il nostro Istituto contribuisce a sensibilizzare docenti, alunni e genitori sui temi della sicurezza online, anche mediante incontri che offriranno occasione di confronto e discussione sui rischi rappresentati dall'uso di cellulari, smartphone e chat line senza

un'adeguata formazione in merito ai rischi derivanti da un uso inappropriato di tali dispositivi. Sul sito scolastico saranno resi accessibili i materiali, tra cui guide in formato pdf e video dedicati alle famiglie e ai ragazzi nella bacheca virtuale del sito di "Generazioni connesse". La scuola darà inoltre ampia diffusione, tramite pubblicazione sul sito, del presente documento di policy per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e favorire un'attiva collaborazione tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi a un uso inappropriato del digitale.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2022)

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2022)

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare

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

La scuola metterà in atto tutte le azioni necessarie per garantire agli studenti l'accesso alla documentazione cercata adottando tutti i sistemi di sicurezza conosciuti per diminuire le possibilità di rischio durante la navigazione. Resta fermo che non è possibile garantire una navigazione totalmente priva di rischi e che la Scuola e gli insegnanti non possono assumersi le responsabilità conseguenti all'accesso accidentale e/o improprio a siti illeciti.

3.2 - Accesso ad Internet

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

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

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli

studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola".

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

L'accesso al sistema informatico per la didattica, server e internet, nel laboratorio multimediale è consentito al personale docente attraverso l'assegnazione di una password da parte dell'Animatore digitale. La password è comune e consente di accedere al server. I docenti registrano il proprio accesso, scrivendo su un registro la data e l'orario di utilizzo del laboratorio. Non vi è un backup dei file elaborati, se non quello operato dai docenti interessati sui supporti rimovibili personali. Le postazioni del laboratorio funzionano come stazioni di lavoro e non come archivi. - E-mail - L'account di posta elettronica è quello istituzionale utilizzato solo dagli uffici amministrativi., sia per la posta in ingresso che in uscita.

L'account di posta elettronica per docenti e alunni quella con dominio comprensivochiancianoterme.it . La posta elettronica è protetta da antivirus, e quella certificata anche dall'antispam.

- Blog e sito web della scuola: La scuola attualmente ha un sito web e una pagina facebook .Tutti i contenuti del settore didattico sono pubblicati direttamente dai compenenti del gruppo TIC, sul sito web pubblica direttamente l'Animatore digitale, che ne valuta con il Dirigente scolastico la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc.

Le principali norme da rispettare sono:

1. L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante;

2. Internet non può essere usato per scopi vietati dalla legislazione vigente;

3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet;

4. E' vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza.Consultare obbligatoriamente prima di installare qualsiasi programma l'animatore digitale, un responsabile di laboratorio o un tecnico per valutarne la compatibilità.

Linee guida di buona condotta dell'utente e buone pratiche nell'uso della rete

- Rispettare la legislazione vigente;

- Tutelare la propria privacy, quella degli altri utenti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui hai accesso;

- Rispettare la cosiddetta netiquette (regole condivise che disciplinano il rapportarsi fra utenti della rete, siti, forum, mail e di qualsiasi altro tipo di comunicazione).

- Controllo della validità e dell'origine delle informazioni a cui si accede o che si ricevono;

-Utilizzo di fonti alternative di informazione per proposte comparate;

- Ricerca del nome dell'autore, dell'ultimo aggiornamento del materiale e di altri possibili link al sito;

- Rispetto dei diritti di autore e dei diritti di proprietà intellettuale.

3.3 - Strumenti di comunicazione online

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

Il nostro istituto dispone di:

- indirizzi mail per insegnanti, personale non docente, le comunicazioni con gli alunni possono avvenire attraverso il registro elettronico e anche mediante l'indirizzo di posta eletrronica gestito tramite G-suite

-Sito web della scuola
Tutti i contenuti didattici, le informazioni alle famiglie, le comunicazioni al personale sono pubblicati sul sito web dell'Istituto, sotto la supervisione della Funzione Strumentale preposta, dell'Animatore Digitale e del D.S., nel rispetto delle norme vigenti sulla privacy e del PTTI d'Istituto.

Social network

L'Istituto ha creato un proprio profilo, autorizzando il personale docente a utilizzarlo per nome e per conto della stessa. I docenti sono tenuti a sottoporre al D.S. i contenuti che intendono pubblicare sulla pagina.

Registro elettronico

Ogni famiglia riceve le credenziali per l'accesso riservato al registro elettronico, in cui il corpo docente è tenuto a registrare assenze, valutazioni, note e osservazioni. L'uso del registro elettronico verrà spiegato alle famiglie nel corso di un incontro orientativo che si terrà alle famiglie all'apertura dell'anno scolastico oltre che ad alcune indicazioni guida da pubblicarsi sul sito della scuola. La pubblicazione delle informazioni attraverso tale strumento assolve l'obbligo di comunicare prontamente ed efficacemente ogni evento riguardante l'alunno/a. Coloro che non possono accedere a Internet e di conseguenza non possono consultare il registro elettronico sono pregati di darne segnalazione al coordinatore del consiglio di classe, che verificherà la trascrizione delle comunicazioni sul diario e la firma dei genitori.

Sicurezza Rete Lan
L'Istituto dispone di una rete locale (rete segreteria) cui accedono i computer dell'amministrazione, isolata dal resto della rete di Istituto (rete didattica). Il collegamento di computer portatili o palmari personali alla rete di Istituto deve essere autorizzato dal Dirigente Scolastico.

La rete interna è protetta da Firewall per quanto riguarda le connessioni con l'esterno. Le postazioni sono protette con sistemi antivirus.
- Sicurezza della rete senza fili (Wireless –WiFi)
L'Istituto dispone di una rete con tecnologia senza fili. L'accesso alla rete wireless è autorizzato ai docenti dal D.S., tramite password e riconoscimento del dispositivo utilizzato. Le regole di comportamento sono analoghe a quelle per la connessione alle reti cablate di Istituto.

3.4 - Strumentazione personale

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

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

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

Per gli studenti: gestione degli strumenti personali

Come da Regolamento d'Istituto agli studenti è vietato l'utilizzo del cellulare all'interno
della scuola. Il collegamento di computer portatili, tablet o altri dispositivi personali alla
rete di Istituto da parte degli studenti può essere consentito in relazione alle attività previste dal PNSD (BYOD) solo per ragioni prettamente scolastiche e sotto la costante supervisione dei docenti.

Per i docenti e per il personale della scuola: gestione degli strumenti personali
- cellulari, tablet ecc…

I docenti e il personale della scuola possono utilizzare cellulari e tablet a scopo personale non durante l'attività didattica o lavorativa.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021).

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto perredigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare incontri per la consultazione degli studenti/studentesse suindicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Adesione al Progetto "Patentino digitale 2020" per il conseguimanto del relativo patentino.Progetto promosso dall' Ufficio scolastico

Regionale, dal Corecom e rivolto alle classi prime della scuola secondaria di primo grado.

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

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse
- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto perredigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

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

Il nostro istituto integra l'offerta formativa con attività finalizzate alla prevenzione e al contrasto del bullismo e del cyberbullismo, nell'ambito delle tematiche afferenti a Cittadinanza e Costituzione per tradurre i "saperi" in comportamenti consapevoli e corretti, indispensabili a consentire alle giovani generazioni di esercitare la democrazia nel rispetto della diversità e delle regole della convivenza civile.

Le indicazioni relative ad un utilizzo sicuro della Rete da parte degli studenti potranno essere oggetto di specifici moduli didattici, da inserire nel Piano dell'Offerta Formativa (POF). La strategia di contrasto dei fenomeni del bullismo dovrebbe essere costituita, quindi, già a partire dalle scuole primarie, da un insieme di misure di prevenzione rivolte agli studenti di varia tipologia. Tra le specifiche azioni da programmare si possono prevedere le seguenti, anche sulla base della attività svolte nell'a.s. 2017/18:

1. coinvolgimento di tutte le componenti della comunità scolastica nella prevenzione e nel contrasto del bullismo e del cyberbullismo, favorendo la collaborazione attiva dei genitori;

2. Attività laboratoriali specifiche sul tema da svolgere in classe ;

3. integrazione della presente policy con il Regolamento di Istituto;

4. comunicazione agli studenti e alle loro famiglie sulle sanzioni previste dal Regolamento di Istituto nei casi di bullismo, cyberbullismo e navigazione online a rischio; 5. somministrazione di questionari agli studenti e ai genitori finalizzati al monitoraggio, anche attraverso piattaforme online con pubblicazione dei risultati sul sito web della scuola, che possano fornire una fotografia della situazione e consentire una valutazione oggettiva dell'efficacia degli interventi attuati;

6. percorsi di formazione tenuti da esperti rivolti ai genitori e ai docenti sulle problematiche del bullismo e del cyberbullismo impostati anche sulla base dell'analisi dei bisogni;

7. utilizzo di procedure codificate per segnalare alle famiglie e/o organismi competenti i comportamenti a rischio.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

"*qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più*

componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo".

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

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
    - Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
    - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Il cyberbullismo è una forma di prepotenza virtuale messa in atto attraverso l'uso di Internet e delle tecnologie digitali. Spesso i termini bullismo e cyberbullismo vengono usati impropriamente e si riconducono ad essi i più svariati episodi di violenza o offese fra ragazzi/e. Bullismo e cyberbullismo hanno, però, connotati ben precisi e non vanno confusi con altre problematiche del mondo giovanile.

Nel 2006 Smith e collaboratori definirono il cyberbullismo come:

"Un atto aggressivo e intenzionale perpetrato da un individuo o da un gruppo, attraverso l'uso delle nuove tecnologie della comunicazione, in modo ripetuto e continuato nel tempo, contro una vittima che non può facilmente difendersi" (in Smith P.K., Mahdavi J., Carvalho C., e Tippett N., An investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbullying. A Report to the Anti-Bullying Alliance, 2006, p.6).

Nel bullismo tradizionale, solitamente, la vittima che viene presa di mira è percepita

come più debole e incapace di difendersi.

Il più forte, quindi, assume atteggiamenti prevaricatori nei confronti del più debole, a partire da una certa “asimmetria di potere”.

el bullismo tradizionale, però, il potere presenta connotati ben precisi, potrebbe essere, ad esempio, di tipo fisico (legato alla forza o alla statura) o sociale (legato alla popolarità), il potere online può derivare semplicemente dal possesso di specifiche competenze o di alcuni contenuti (immagini, video, confessioni) che potrebbero essere utilizzati per danneggiare la vittima.

Solitamente, quando si parla di cyberbullismo o di bullismo è necessario che vittima e bullo/cyberbullo siano minori o comunque adolescenti (sono esclusi, quindi, dalla definizione episodi di prevaricazione che avvengono fra adulti o fra un adulto e un minore).

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

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

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

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

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

Il discorso dell’odio si manifesta con un ampio spettro di azioni: sebbene tutte le espressioni che istigano all’odio meritino di essere classificate come malvagie, ne

esistono alcune che possono essere peggiori di altre. È utile, quindi, prendere in considerazione alcuni aspetti:

Il contenuto e il tono

Certe espressioni di odio sono più estreme, utilizzano termini più insultanti e possono perfino istigare altri ad agire. All'altra estremità della scala, troviamo insulti più moderati o generalizzazioni eccessive, che presentano certi gruppi o individui sotto una cattiva (e perfino sotto falsa) luce.

L'intenzione degli autori degli insulti

Ci può capitare di offendere gli altri senza volerlo, e poi di pentircene, e perfino di ritirare quanto abbiamo detto. Nei due esempi seguenti, entrambe le affermazioni sono intolleranti e sgradevoli, ma una è stata scritta con l'intenzione di offendere e fare del male.

I bersagli o i bersagli potenziali

Alcuni gruppi, o individui, possono essere più vulnerabili di altri alle critiche. Può dipendere dal modo in cui sono globalmente considerati nella società, o da come sono rappresentati nei media, oppure dalla loro situazione personale, che non permette loro di difendersi efficacemente. L'esempio qui sotto mostra come la stessa espressione, applicata a gruppi diversi, possa avere un impatto molto diverso. Quella di destra rischia di essere molto più pregiudizievole.

Il contesto

Il contesto di una particolare espressione di odio è legato talvolta a circostanze storiche e culturali specifiche. Può includere altri fattori, come il mezzo utilizzato e il gruppo preso di mira, le tensioni o i pregiudizi esistenti, l'autorità del suo autore, etc.

L'impatto o l'impatto potenziale

L'impatto reale o potenziale esercitato sugli individui, sui gruppi o sull'insieme della società è una delle principali considerazioni da tenere presenti. Spesso, le ripercussioni negative subite dall'individuo o dal gruppo si rivelano più importanti della valutazione dell'episodio da parte di osservatori esterni.

Come prevenirlo

Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono quindi un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete.

Occorre in tal senso fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, e promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network.

4.4 - Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale?

La dipendenza da Internet, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica che deve attenzionare il fenomeno e fornire gli strumenti agli studenti e alle studentesse affinché questi siano consapevoli dei rischi che comporta l'iperconnessione.

La scuola offirà dei percorsi di formazione per indicare strategie per un uso più consapevole delle tecnologie per favorire il "benessere digitale", cioè la capacità di creare e mantenere una relazione sana con la tecnologia.

4.5 - Sexting

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

Il sexting (abbreviazione di sex – sesso e texting – messaggiare, inviare messaggi) indica l'invio e/o la ricezione di contenuti (video o immagini) sessualmente espliciti che ritraggono se stessi o gli altri. Questi contenuti possono diventare materiale di ricatto assumendo la forma di "revenge porn" letteralmente "vendetta porno" fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte (la Legge 19 luglio 2019 n. 69, all'articolo 10 ha introdotto in Italia il reato di revenge porn, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti.)

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

4.6 - Adescamento online

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

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

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

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

Potenziali vittime dell'adescamento online possono essere sia bambini che bambine, sia ragazzi che ragazze. Il fenomeno, infatti, non conosce distinzione di genere. Gli adolescenti sono particolarmente vulnerabili, poiché si trovano in una fase della loro vita in cui è molto importante il processo di costruzione dell'identità sessuale. Anche per questo potrebbero essere aperti e curiosi verso nuove esperienze e, talvolta, attratti da relazioni intime e apparentemente rassicuranti. In questa fase è importante, infatti, il bisogno di avere attenzioni esclusive da un'altra persona, di ottenere rinforzi esterni di approvazione per il proprio corpo e la propria immagine.L'adescamento, quindi, non avviene apparentemente con una dinamica violenta, ma il "prendersi cura" del minore rappresenta la conditio per carpirne la fiducia ed instaurare una relazione a

sfondo erotico. Può capitare che l'adescatore si presenti al minore sotto falsa identità, fingendo quindi di essere un'altra persona così da attirare maggiormente l'attenzione del minore (ad esempio, potrebbe fingersi un talent scout del mondo dello spettacolo alla ricerca di volti nuovi).

Per riconoscere un eventuale caso di adescamento online è importante prestare attenzione a piccoli segnali che possono essere indicatori importanti, come ad esempio un cambiamento improvviso nel comportamento di un minore. **A seguire, alcuni segnali e domande che potrebbero esserci di aiuto:**

- Il minore ha conoscenze sessuali non adeguate alla sua età?
- Venite a conoscenza di un certo video o di una foto che circola online o che il minore ha ricevuto o filmato, ma c'è imbarazzo e preoccupazione nel raccontarvi di più…
- Il minore si isola totalmente e sembra preso solo da una relazione online?
- Ci sono prese in giro e allusioni sessuali verso un bambino/ragazzo in particolare?

Come prevenirlo

Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità.

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 e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è).

4.7 - Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, **concrete o simulate** o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

La legge n. 269 del 3 agosto 1998 *"Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù", introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella* ***legge n. 38 del 6 febbraio 2006*** *"Disposizioni in materia di lotta contro lo sfruttamento*

sessuale dei bambini e la pedopornografia anche a mezzo Internet", segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di "pornografia minorile virtuale" (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

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

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione **"Segnala contenuti illegali"** (Hotline).

Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children.

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolte/i in comportamenti sessualmente espliciti, concrete o simulate o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

Qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione "Segnala contenuti illegali" (Hotline). Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I

due servizi messi a disposizione dal Safer Internet Centre sono il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children. Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia. L'intento è quello di facilitare il processo di rimozione del materiale stesso dalla Rete e allo stesso tempo consentire le opportune attività investigative finalizzate ad identificare chi possiede quel materiale, chi lo diffonde e chi lo produce, ma, soprattutto e primariamente, ad identificare i minori abusati presenti nelle immagini e video, assicurando la fine di un abuso che potrebbe essere ancora in corso e il supporto necessario.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2020/2021).

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

x 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.

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

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

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

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

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

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire).

Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).

Nelle procedure:

- sono indicate le **figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso**.
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

Inoltre, la scuola **individua le figure che costituiranno un team** preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la **collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio** (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica.

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e

studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

A seguire, le problematiche a cui fanno riferimento le procedure allegate:

- **Cyberbullismo**: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online**: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting**: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per

segnalare la presenza di materiale pedopornografico online.

Intervenire: sì o no? SEMPRE. Siamo chiamati a garantire il benessere dei nostri alunni, oltre che a trasmettere conoscenze. Se un alunno ha confidato qualcosa che lo preoccupa di ciò che accade online, significa che si fida di noi e pensa che si abbiano le risorse per aiutarlo.

Come accorgersi se un alunno è coinvolto in casi di (cyber)bullismo? Accorgersi di episodi di (cyber)bullismo non è sempre facile perché le prevaricazioni avvengono in luoghi virtuali in cui gli adolescenti si ritrovano. Per cui è necessario cogliere i segnali che i ragazzi ci lanciano quando si trovano in una situazione di disagio o di difficoltà. Una "prova" di quanto riferito può essere presente nella memoria degli strumenti tecnologici utilizzati, può:

1) essere mostrata spontaneamente dall'alunno,

2) essere presentata da un reclamo dei genitori,

3) essere notata dall'insegnante che si accorge dell'infrazione in corso. I contenuti "pericolosi" comunicati/ricevuti a/da altri, messi/scaricati in rete, ovvero le tracce che possono comprovare l'utilizzo incauto o scorretto degli strumenti digitali utilizzabili anche a scuola attualmente dai minori(l'eventuale telefonino/smartphone personale e il pc collegato a internet) per gli alunni possono essere i seguenti:

a) Contenuti afferenti alla privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, furto, appropriazione, uso e rivelazione ad altri di informazioni personali come le credenziali d'accesso all'account e-mail, social network ecc.);

b) Contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, offese e insulti tramite messaggi di testo, email, pubblicati su social network o tramite telefono ,foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);

c) Contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, diffusione di foto o video che ritraggono situazioni intime, violente o spiacevoli tramite il cellulare, siti web o social network ,foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

5.2. - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

- CASO A (SOSPETTO) – Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.
- CASO B (EVIDENZA) – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

Per tutti i dettagli fate riferimento agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

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

5.2 Come segnalare : procedure operative e strumenti PROCEDURE OPERATIVE IN CASO DI SOSPETTO O EVIDENTE CASO DI CYBERBULLISMO PREVISTE NEL

NOSTRO ISTITUTO

1. Ascolta: chiedigli/le cosa puoi fare per lui/lei e cosa desidera che accada;

2. Se l'alunno ci porge spontaneamente le prove i docenti possono consultarle e condividerle con lui.

3. Avvisare e comunicare immediatamente l'accaduto al Dirigente scolastico , al vicario e al referente cybebullismo

4. Avere un colloquio con la "vittima" o accogliere la sua segnalazione alla presenza di chi ha rilevato il caso, del referente del cybebbullismo e della dirigente scolastica (o vicario)

5. Assicurarsi che l'alunno vittima salvi nel suo telefono ogni messaggio, voce/testo/immagine, conservando così il numero del mittente.

6. Avvisare telefonicamente i genitori della vittima che conservi e condivida il contenuto e fare in modo che la famiglia si accerti della segnalazione ricevuta. Fare in modo che la famiglia si accerti della segnalazione

7. Conservare la prova, per il genitore, è utile per far conoscere l'accaduto in base alla gravità ai genitori degli alunni bulli, al Dirigente scolastico e per le condotte criminose alla polizia.

8. Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno,quantunque riferite a fatti accaduti al di fuori del contesto scolastico, le notizie raccolte sono comunque comunicate ai genitori e per fatti rilevanti anche al Dirigente scolastico; per quelle criminose, anche alla polizia.

9. Accertarsi del danno e avere copia o screenshot della conversazione dal genitore della vittima.

10. Intervenire con il protocollo di intervento (ALLEGATO 3): agite per ridare benessere al tuo/a alunno/a.

11. Avere un colloquio con il "bullo/bulli", alla presenza di chi ha rilevato il caso, del referente del cybebbullismo e della dirigente scolsastica (o vicario) 12. Chiamare per un colloquio i genitori del "bullo o dei bulli", per condividere la gravità della situazione rilevata e comunicare le successive azioni da mettere in atto 13. In base all'urgenza le comunicazioni formali possono essere precedute da quelle informali, effettuate per le vie brevi.

14. fermare immediatamente l'abuso

15. Consultare il numero 1.96.96, soprattutto nei casi gravi o complessi .

16. Convocare il consiglio di classe che nel caso sia necessario applichi eventuali sanzioni

17. Applicare la sanzione comunicandolo ai genitori

18. Avvisare in casi gravi la Polizia Postale e delle Comunicazioni

---

5.3. - Gli attori sul territorio

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

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

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

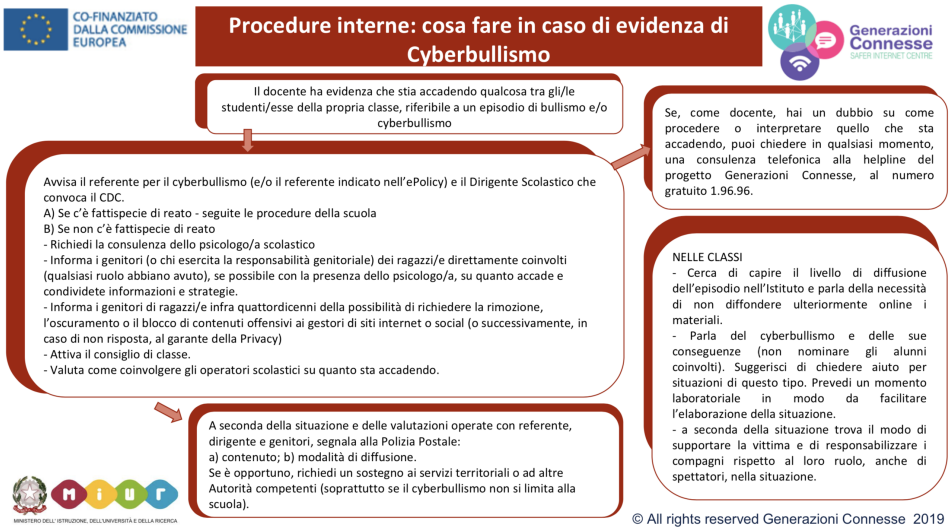
- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.

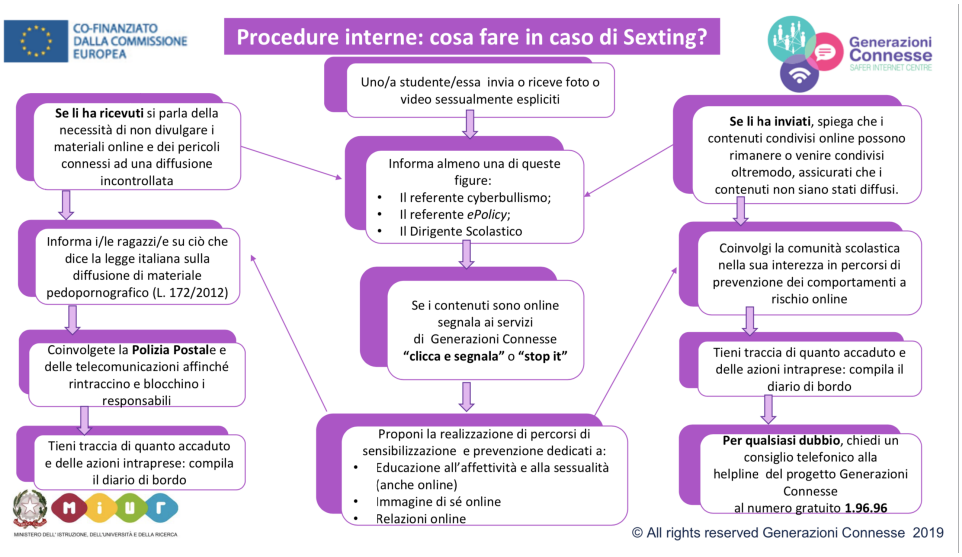
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

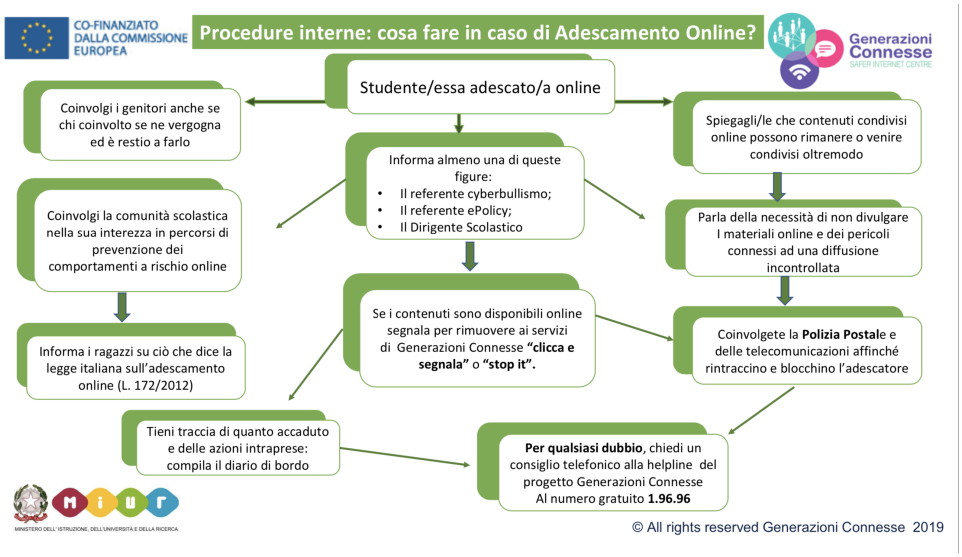
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



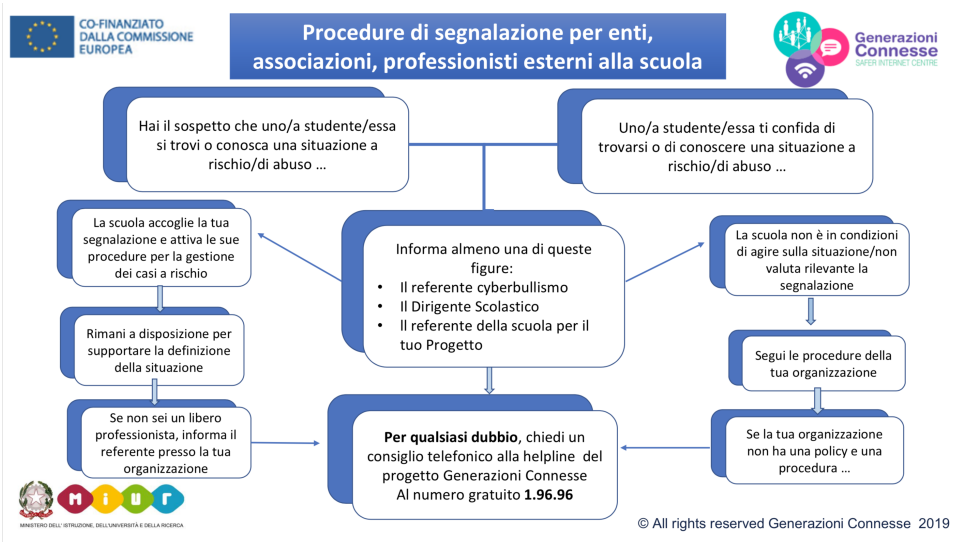
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

LINEE GUIDA PER I RAGAZZI 1. FAI ATTENZIONE perché rimane sempre traccia di quello che posti o scrivi su internet; 2. STAI ATTENTO a chi vuol sapere troppe cose. Non dare a nessuno informazioni personali e della famiglia (nome, cognome, età, indirizzo, numero di telefono, nome e orari della scuola, nome degli amici). 3. CHIEDI SEMPRE IL PERMESSO prima di inviare o pubblicare su una chat , un social o su una app, qualsiasi materiale in cui ci siano altre persone (foto, video, commenti, etc) ; 4. CHIEDITI se vorresti esserci tu al suo posto quando fai commenti , metti foto o video di/su altri. 5. NON RISPONDERE alle offese ed agli insulti; 6. CONSERVA E SALVA le comunicazioni offensive, ti potrebbero essere utili per dimostrare quanto ti è accaduto; 7. Se ricevi materiale offensivo (e-mail, sms, mms, video, foto, messaggi vocali) NON DIFFONDERLO:potresti essere accusato di cyberbullismo; 8. Rifletti prima di inviare: ricordati che tutto ciò che invii su internet diviene pubblico e rimane per SEMPRE; 9. Quando sei connessi alla rete RISPETTA SEMPRE GLI ALTRI,ciò che per te è un gioco può rivelarsi offensivo per qualcun altro; 10.SE PARTECIPI A GRUPPI in cui leggi offese , dillo ai tuoi genitori o insegnanti , fai screenshot , salva il materiale e poi esci dal gruppo. 11.Riferisci al tuo insegnante o ai tuoi genitori se qualcuno ti invia immagini che ti infastidiscono e non rispondere; riferisci anche al tuo insegnante o ai tuoi genitori se ti capita di trovare immagini di questo tipo su Internet; 12.Ricordati che se qualcuno ti offende pesantemente puoi ricorrere alla Dirigente, al referente bullismo, ai tuoi genitori e anche alla Polizia postale 13.Ricordati che è facile mentire

su internet. Alcune persone possono fingersi per quello che non sono. Anche le immagini web possono essere false. 14.PENSA prima di mettere qualsiasi cosa su internet. NON pubblicare , inviare o condividere materiale imbarazzante o dannoso e inopportuno. 15.Tutti quelli che osservano senza far nulla diventano corresponsabili delle azioni del cyber bullo; mettere un "like" su un social o condividere o commentare foto o video sottopone chi lo fa a una responsabilità maggiore. 42 16.Rispettate la privacy altrui. State attenti soprattutto a non pubblicare informazioni personali relative ad altri (comprese immagini, foto o video) senza il loro consenso. 17.La privacy non vi protegge se commettete atti di cybebullismo su qualcuno (offese, messaggio volgari, foto private e intime et) 18.Utilizza password sicure (lunghe con numeri e lettere) tienile riservate. Se vedi cose strane cambiale. 19.Non scaricare - senza parlarne con gli adulti - loghi, suonerie, app, immagini o file in genere, sia da Internet che come allegati a messaggi di posta elettronica, che possono creare intromissioni nel computer, ovvero possono comportare costi o addebiti indesiderati.

LINEE GUIDA PER I GENITORI Consigli per difendere i propri figli dai pericoli legati all'uso delle nuove tecnologie Molti bambini utilizzano internet già durante i primi anni della scuola primaria (6-7 anni). È importante sottolineare che è fondamentale l'accompagnamento all'utilizzo di internet da parte di un adulto (genitore, insegnante, educatore) in relazione all'età del bambino.I bambini al di sotto dei 10-11 anni, in genere, non avendo ancora sviluppato le capacità di pensiero critico necessarie, non sono in grado di esplorare il web da soli. scaricano musica, utilizzano motori di ricerca per trovare informazioni, visitano siti, inviano e ricevono sms, la posta elettronica e i giochi online. La supervisione degli adulti è quindi fondamentale anche in questa fase, poiché una maggior conoscenza e consapevolezza legate alla crescita non mettono comunque al riparo dai rischi della Rete. Chiedete ai vostri figli di essere informati rispetto alla loro attività in rete: cosa fanno e con chi stanno condividendo Ricordatevi che siete responsabili fino ai 14 anni dell'utilizzo che fanno del loro samrtphone; Utilizzate app di condivisione (tipo whatsapp) tra genitori in modo consono allo scopo per cui vengono creati i gruppi, utilizzando modalità comuncative appropriate; Stabilite i tempi di utilizzo del computer e del collegamento in rete secondo l'età del minore; Condividete con lui le raccomandazioni e le regole di utilizzo dello smartphone per un uso consapevole e corretto; Creare un rapporto di dialogo con il minore, essere disponibili, farsi raccontare dei suoi contatti e dei suoi interessi in rete (siti visitati, chat, ricerche e scoperte effettuate); Di tanto in tanto controllare i contenuti postati su Internet dai vostri figli.; Non lasciare da soli i ragazzi nell'utilizzo dello smartphone, soprattutto se frequentano la primaria Fate in modo di non lasciare a loro disposizione lo smartphone di notte; Utilizzate applicativi che possano aiutarvi nel controllo dello smartphone Parlate apertamente dei rischi che si possono correre utilizzando internet e whatsapp; Controllate la cronologia o gli applicativi scaricati sul loro smartphone; Dite di non dare mai dati personali in

rete; Ditegli di non rispondere agli insulti perché cosi diventa anche lui colpevole; Ricordagli che tutti i cellulari o pc lasciano una traccia che può essere trovata dalla Polizia; 44 Ricordargli che le cose scritte o alcune fotografie , POSSONO FAR PIU' MALE perché rimangono SEMPRE; Fate presente che molti comportamenti illeciti che loro conosco nel reale(insultare, offendere , fotografare di nascosto, accedere illecitamente ad un servizio, etc) lo sono anche nel virtuale; Fate presente e insistete ch qualcosa messo su internet è incancellabil Salvate sul computer il materiale che può fungere da prova (per esempio screenshot, conversazioni in chat e immagini) e subito dopo, se possibile, cancellare – o far cancellare dal gestore della piattaforma – tutti i contenuti in rete Se sono coinvolti compagni di scuola, i genitori dovrebbero rivolgersi agli insegnanti e, laddove presente, allo psicologo scolastico per valutare se sporgere denuncia presso la polizia LINK www.commissariatops.it www.generazioniconnesse.it

Il nostro piano d'azioni

L'Istituto comprensivo si propone di :

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

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

- Organizzare uno o più incontri 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 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.