MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITA' E DELLA RICERCA
UFFICIO SCOLASTICO REGIONALE PER LA SICILIA
ISTITUTO COMPRENSIVO STATALE "L. DA VINCI- G. CARDUCCI" PALERMO
Via Ferdinando Di Giorgi, 48, 90145 (PA)
www.icdavincicarducci.gov.it

POLICY DI E-SAFETY
A.S. 2017-18

1. INTRODUZIONE

Scopo della policy

Il presente documento viene predisposto in riferimento alle indicazioni riportate nelle "LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrasto al bullismo e cyberbullismo" elaborate dal Ministero dell'Istruzione, dell'Università e della Ricerca (aprile 2015), in collaborazione con "Generazioni Connesse" e il Safer Internet Center per l'Italia, programma comunitario istituito dal DFC Europeo e dal Consiglio dell'Unione.
L'impegno educativo del nostro Istituto per la realizzazione del successo formativo dei singoli alunni, consiste nel garantire l'utilizzo di Internet ed
altre tecnologie digitali orientato a:
-elevare gli standard educativi e promuovere i risultati degli studenti;
-rendere l'apprendimento più coinvolgente, partecipato e proficuo;
-consentire agli studenti di accedere ad un'ampia gamma di conoscenze in maniera consapevole e sicura.
In tale prospettiva la scuola adotta un protocollo di E-safety, che prevede la formazione dei docenti, del personale amministrativo, degli alunni e delle loro famiglie per un utilizzo corretto e sicuro delle infrastrutture digitali, delle nuove tecnologie della scuola e di quelle personali.

Ruoli e responsabilità

Il Dirigente Scolastico è responsabile della presentazione di questo documento all'attenzione del Consiglio di Istituto e al Collegio dei Docenti; ne valuta l'efficacia e ne indirizza/monitora l'attuazione, anche in collaborazione con personale scolastico, enti locali e stakeholder territoriali. A tale scopo necessita di ricevere tempestive informazioni sulle violazioni al presente regolamento o eventuali problemi attualmente non noti dal corpo docente o dal personale ATA che ne vengano a conoscenza.
L'animatore digitale favorisce l'uso delle tecnologie nella didattica e potenzia le competenze dei docenti e degli studenti in campo digitale. Egli collabora strettamente con tutto il personale docente per sviluppare la necessaria sensibilità nell'utilizzo di Internet e delle altre tecnologie digitali nella didattica.
I docenti promuovono, coordinano e monitorano l'accesso alla rete e l'utilizzo delle altre tecnologie da parte degli studenti durante l'orario scolastico.

I genitori sono tenuti a prestare la massima attenzione ai principi e alle regole contenute nel presente documento impegnandosi a farle rispettare ai propri figli anche in ambito domestico, assistendo i minori nel momento dell'utilizzo della rete e ponendo in atto tutti i sistemi di sicurezza che aiutino a diminuire il rischio di imbattersi in materiale indesiderato. In quanto tutori legali, hanno la responsabilità ultima per un non corretto utilizzo degli strumenti personali (cellulari, video-cellulari, connessioni ad Internet).
Il Direttore dei servizi generali e amministrativi, nei limiti delle risorse finanziarie disponibili, garantisce il funzionamento sicuro e non soggetto a uso improprio dell'infrastruttura tecnica della scuola, il funzionamento dei diversi canali di comunicazione della scuola (circolari, Registro Elettronico e Sito web), all'interno e all'esterno con le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore Digitale riguardanti l'uso delle tecnologie digitali e i rischi ad essi connessi.
Il personale ATA è tenuto a conoscere la presente policy, a segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'animatore digitale per le opportune indagini, azioni o sanzioni.
Le alunne/gli alunni sono responsabili per l'utilizzo corretto dei sistemi informatici e della tecnologia digitale in accordo con i termini previsti da questa policy.

Condivisione e comunicazione della policy all'intera comunità scolastica

l'Istituto si impegna ad adottare la presente policy allo scopo di condividere regole comuni per l'utilizzo sicuro di Internet sia a casa che a scuola e pubblica il presente documento sul sito della scuola. La scuola promuove eventi e/o dibattiti informativi e formativi, in momenti diversi dell'anno, rivolti a tutto il personale, agli alunni e ai loro genitori, con il coinvolgimento di esperti, sui temi oggetto di questo documento.

Gestione delle infrazioni alla policy

Tra le misure di prevenzione che la scuola mette in atto ci sono, inoltre, azioni finalizzate a promuovere una cultura dell'inclusione, del rispetto dell'altro e delle differenze così che l'utilizzo di Internet e dei cellulari oltre che collocarci all'interno di un sistema di relazioni, ci renda consapevoli di gestire con un certo grado di trasparenza i rapporti che si sviluppano in tale ambiente, giungendo a riconoscere e gestire le proprie emozioni. A tal proposito si potrà attivare uno "Sportello di ascolto" rivolto a tutti gli alunni, articolato in colloqui individuali e/o collettivi, al fine di migliorare il benessere personale e scolastico mediante un'attività di supporto della sfera emotiva, relazionale e comportamentale. Si può prevedere al suo interno, anche uno spazio riservato ai docenti e genitori al fine di individuare strategie efficaci per affrontare problematiche tipiche dell'età adolescenziale.

Monitoraggio dell’implementazione alla policy e suo aggiornamento

La scuola opera in stretto collegamento con le forze dell'ordine, con la Procura della Repubblica, con istituzioni del settore educativo, per mettere in campo strategie di prevenzione al cyber-bullismo e interventi di recupero nel caso in cui vengano individuati tali fenomeni, informando i genitori/tutori e chiedendo la loro collaborazione anche qualora gli episodi si siano verificati al di fuori delle attività didattiche.

La scuola accoglie minori “nativi digitali” che fin dall'infanzia sono esposti a rischi di cui sono inconsapevoli, pertanto attua attività di prevenzione, controllo e formazione di allieve, allievi e famiglie allo scopo di ridurre al minimo l'occorrenza di atti che non solo creano disagio nella comunità scolastica, ma possono configurarsi come reati.

Le nuove tecnologie dell’informazione e della comunicazione, così diffuse nella nostra società, nella scuola rappresentano un mezzo per un rapporto più efficiente e trasparente con il territorio e sono strumenti per facilitare e supportare una didattica motivante e innovativa.

L’accesso sicuro ad Internet e il corretto utilizzo delle sue risorse, è un diritto-dovere degli studenti e degli insegnanti. Il PTOF d’Istituto individua nell’uso delle TIC (Tecnologie dell’Informazione e della Comunicazione) un supporto essenziale nei processi di insegnamento/apprendimento e l’impiego consapevole delle risorse digitali coinvolge tutte le componenti della comunità scolastica.

Per evitare che il presente documento rappresenti un mero atto formale, esso si pone come base di partenza per una serie di azioni e iniziative; a partire dalla pubblicazione sul sito della scuola, si possono ipotizzare per esempio:

Per il corpo docente:

- discussione collegiale sui contenuti, sulle pratiche indicate e su come inserire nel curricolo le tematiche di interesse della policy;
- un confronto collegiale, su base annuale, circa la necessità di apportare modifiche e miglioramenti alla policy vigente;
- elaborazione di protocolli condivisi di intervento.

Per i genitori:

- l'organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare.

Per la componente studentesca:

- la discussione in classe della policy nei primi giorni di scuola, con particolare riguardo al protocollo di accoglienza per le nuove classi prime;

In particolare gli studenti e le studentesse sono tenuti a:

- non utilizzare dispositivi personali durante le attività didattiche se non espressamente consentito dal personale docente:
- avere una buona comprensione delle possibilità di ricerca sul web e della necessità di evitare il plagio, rispettare le normative sul diritto d'autore, non diffondere dati personali;
- conoscere e comprendere le politiche sull'uso di dispositivi mobili e di macchine fotografiche digitali;

- capire le politiche di utilizzo delle immagini ed essere consapevoli del significato e della gravità del cyber-bullismo.
- capire l'importanza di adottare buone pratiche di sicurezza informatica in tutti i momenti della vita, a tutela dell'incolumità propria e altrui e per evitare di perpetrare reati punibili sia a livello scolastico sia da parte della magistratura.

Integrazione della policy con i regolamenti esistenti

Nel corso degli anni, con i finanziamenti del Fondo Europeo di Sviluppo Regionale-FSE e del MIUR, la scuola si è dotata di strumenti tecnologici ed ha favorito la formazione del personale per far crescere le competenze professionali nell'impiego delle nuove tecnologie. L'utilizzo e il corretto funzionamento delle aule e delle postazioni informatiche, le prenotazioni, la tracciabilità delle apparecchiature, la segnalazione di malfunzionamenti è disciplinato da un Regolamento nell'ottica della migliore collaborazione collegiale.
Gli insegnanti sono responsabili delle TIC nell'ambito dell'attività didattica: è consentito l'accesso alle postazioni computer singole o in rete dell'Istituto scolastico negli orari di apertura della scuola per compiti connessi allo svolgimento delle proprie mansioni. Agli alunni è consentito l'accesso in orario scolastico solo ed esclusivamente se accompagnati dal docente di riferimento, il quale controllerà che l'utilizzo avvenga secondo le modalità previste dal regolamento dei laboratori.
I docenti hanno la responsabilità di guidare gli studenti nelle attività on-line, di stabilire obiettivi chiari per un uso consapevole di internet, di prevenire il verificarsi di situazioni critiche, utilizzando percorsi guidati in riferimento all'obiettivo di arricchire ed ampliare le attività didattiche, secondo quanto prevede il curricolo scolastico, l'età e la maturità degli studenti.

2. FORMAZIONE E CURRICOLO

Curricolo sulle competenze digitali degli studenti

La competenza digitale, trasversale ad ogni altra competenza, risulta funzionale all'esercizio della cittadinanza; consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione per lo studio, 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
AREE DI COMPETENZA DIGITALE
1. INFORMAZIONE: identificare, localizzare, recuperare, conservare, organizzare e analizzare le informazioni digitali, giudicare la loro importanza e lo scopo.
2. COMUNICAZIONE: comunicare in ambienti digitali, condividere risorse attraverso strumenti on-line, collegarsi con gli altri e collaborare attraverso strumenti digitali, interagire e partecipare alle comunità e alle reti.
3. CREAZIONE DI CONTENUTI: creare e modificare nuovi contenuti (da elaborazione testi a immagini e video); integrare e rielaborare le conoscenze e i

contenuti; produrre espressioni creative, contenuti mediali e programmare; conoscere e applicare i diritti di proprietà intellettuale e le licenze.
4. SICUREZZA: protezione personale, protezione dei dati, protezione dell'identità digitale, misure di sicurezza, uso sicuro e sostenibile.
5. PROBLEM-SOLVING: identificare i bisogni e le risorse digitali, prendere decisioni informate sui più appropriati strumenti digitali secondo lo scopo o necessità, risolvere problemi concettuali attraverso i mezzi digitali, utilizzare creativamente le tecnologie, risolvere problemi tecnici, aggiornare la propria competenza e quella altrui.

Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica.

Il corpo docente ha partecipato a corsi di formazione anche nell'ambito di piani nazionali, oltre che ad iniziative organizzate da istituzioni del territorio o dalle scuole associate in rete e possiede generalmente una discreta base di competenze e nel caso delle figure di sistema, anche certificate.
Il percorso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica, non esauribile nell'arco di un anno scolastico, deve prevedere corsi di aggiornamento online, momenti di autoaggiornamento, momenti di formazione personale o collettiva anche all'interno dell'istituto, con la condivisione delle conoscenze tra i singoli e con il supporto dell'Animatore digitale, la partecipazione alle iniziative promosse dall'Amministrazione centrale e dalle scuole polo; comprende altresì la fruizione dei materiali messi a disposizione dall'Animatore stesso sulle bacheche virtuali appositamente create.
Sarà implementata una bacheca online per la messa a disposizione e la condivisione di materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di internet, fruibili attraverso l'inserimento di una password cliccando su area riservata accessibile dalla homepage del sito scolastico (www.icdavincicarducci.gov.it). Qui è possibile trovare materiali informativi sulla sicurezza in internet per l'approfondimento personale, per le attività con gli studenti e gli incontri con i genitori, costituiti da guide in pdf, video, manuali a fumetti, link a siti specializzati e contributi della Polizia di Stato, dell'Arma dei Carabinieri, di Telefono Azzurro, dal sito "Generazioni connesse", ecc.; il sito inoltre riporta una sitografia selezionata cui riferirsi per sviluppare attività didattiche innovative.

Sensibilizzazione delle famiglie.

L' Istituto attiverà iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine sono previsti incontri fra docenti e genitori per la diffusione del materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati e dalle forze dell'ordine.
Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del

cyberbullismo. Sul sito scolastico e sulla relativa bacheca virtuale relativa a "Generazioni connesse" saranno messi in condivisione materiali dedicati ad alunni e alle famiglie come guide in formato .pdf e video che possono fornire spunti di approfondimento e confronto.
La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento (Policy e-safety) per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e prevenire i rischi legati a un utilizzo non corretto di internet.

3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA.

Accesso ad internet: filtri, antivirus e sulla navigazione.

L'accesso a internet è possibile e consentito per la didattica nei laboratori multimediali e nelle aule. Solo il docente può consentire agli alunni di accedere a internet. L'accesso è per tutti schermato da filtri che dal server impediscono il collegamento a siti appartenenti a black list o consentono il collegamento solo a siti idonei alla didattica. Le postazioni degli alunni (client) sono occasionalmente utilizzate anche dai docenti, quando questi si servono dei laboratori. I docenti hanno piena autonomia nel collegamento ai siti web.

Gestione accessi (password, backup, ecc.).

L'accesso al sistema informatico per la didattica, server e internet, è consentito al personale docente. Nelle aule informatiche 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 solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. L'eventuale invio o ricevimento di posta a scopi didattici avviene solo su autorizzazione del Dirigente scolastico. La posta elettronica è protetta da antivirus, e quella certificata anche dall'antispam.

Sito web della scuola

Tutti i contenuti del settore didattico sono pubblicati direttamente e sotto supervisione dell'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.

Social Learning

Attualmente nella didattica alcuni docenti utilizzano esclusivamente social learning e i gruppi classe creati sono supervisionati dal docente.

Protezione dei dati personali

A partire dal 25 maggio 2018 è direttamente applicabile in tutti gli Stati membri il Regolamento Ue 2016/679, noto come GDPR (General Data Protection Regulation) – relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali.
La scuola intende affrontare le priorità operative come da Regolamento Eu 2016/279:
-La designazione in tempi stretti del Responsabile della protezione dei dati;
-L'istituzione del Registro delle attività di trattamento;
-La notifica dei data breach.
Il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Tutto il personale incaricato riceve poi istruzioni particolareggiate applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi.
Viene inoltre fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori.

4-STRUMENTAZIONE PERSONALE

Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc…

Durante le ore delle lezioni è consentito l'utilizzo del cellulare solo in caso di urgenza per comunicazioni tra gli alunni e le famiglie, su autorizzazione del docente che verifica l'identità dell'interlocutore.
È consentito l'uso di altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili, su autorizzazione dei genitori e con il controllo delle attività svolte da parte del docente.

Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc…

Durante le ore delle lezioni non è consentito l'utilizzo del cellulare, mentre è consentito l'uso di altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili.
Durante il restante orario di servizio è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente mentre è permesso l'uso di altri dispositivi elettronici personali per attività funzionali all'insegnamento, ad integrazione di quelli scolastici disponibili.

Per il personale della scuola: gestione degli strumenti personali – cellulari

Durante l'orario di servizio al restante personale scolastico è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente

Prevenzione, rilevazione e gestione dei casi

Gli utenti non dovranno:
• Visitare un sito internet, scrivere, inviare, scaricare, caricare o trasmettere, materiali, osservazioni, proposte o commenti che contengano o si riferiscano a:
immagini indecenti di bambini
discriminazioni di ogni genere o incitamento all'odio razziale o religioso o
atti illegali o qualsiasi altra informazione che possa essere offensiva per i coetanei o colleghi.
Accessi occasionali che comportino la navigazione intenzionale di siti web, newsgroup e gruppi online che contengono il seguente materiale, verranno segnalati alla polizia:
• Materiale per adulti che viola la legge sulle pubblicazioni oscene
• Materiale razzista o anti-religioso
• Violenza in generale
• Uso e abuso di farmaci
• Pirateria informatica
• Rivelare o pubblicizzare informazioni riservate o personali, che comprendono: informazioni finanziarie, informazioni personali, banche dati e le informazioni in esso contenute, codici di accesso alla rete o ai computer e le relazioni commerciali;
• Interferire intenzionalmente con il normale funzionamento della connessione internet, compresa la diffusione di virus informatici e il traffico di rete elevato (invio o ricezione di file di grandi dimensioni o l'invio e la ricezione di un gran numero di piccoli file o qualsiasi attività che provochi la congestione della rete) che ostacoli gli altri nel loro utilizzo di Internet;
• Usare Internet per sollecitare, illustrare opinioni personali o rivelare informazioni riservate tali da essere considerate inadeguate.
• Trasmettere materiale commerciale o pubblicitario non richiesto ad utenti o ad organizzazioni collegate ad altre reti, a meno che il materiale sia incorporato all'interno, o faccia parte di un servizio al quale l'utente ha scelto di iscriversi.
• Intraprendere una delle seguenti attività:

- rovinare o cancellare i dati di altri utenti;
-violare la privacy di altri utenti;
-interrompere il lavoro di altri utenti;
-utilizzare le tecnologie mobili 3G o i servizi di telefonia Internet in alcun modo per intimidire, minacciare o danneggiare gli altri.

Prevenzione

Vengono messe in atto le seguenti azioni atte a prevenire un utilizzo scorretto o pericoloso della rete:
a- Attivazione di un filtro per proteggere la navigazione degli alunni a scuola
b- Dotazione di un antivirus attivo e sempre aggiornato (anche gratuito) per tutti i dispositivi
c- Aggiornamento costante dei sistemi operativi

Rischi

I rischi effettivi che si possono correre a scuola nell'utilizzo delle TIC da parte degli alunni derivano da un uso non corretto del telefono cellulare personale, dello smartphone o dei pc della scuola collegati alla rete.
l laboratorio informatico e con un accesso non controllato a internet.

Azioni

Le azioni previste di prevenzione nell'utilizzo delle TIC sono le seguenti:
Informare e formare i docenti, i genitori, il personale ATA e gli studenti sui rischi che un uso non sicuro delle nuove tecnologie può favorire;
Fornire ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori (es. liberatoria per la pubblicazione delle eventuali foto, immagini, testi e disegni relativi al proprio/a figlio/a);
Non consentire l'utilizzo del cellulare personale degli alunni a scuola, in quanto per assolvere a ogni comunicazione urgente con i genitori o con chi ne fa le veci è sempre disponibile il telefono della scuola supervisionato dal personale addetto al centralino, che prima di passare la telefonata si accerta dell'identità dell'interlocutore;
Consentire l'utilizzo del cellulare sono in casi particolari ed eccezionali, ad esempio quando ci si trova fuori dal contesto scolastico durante una visita guidata, e comunque sotto la supervisione dell'insegnante, che si accerta preventivamente dell'identità dell'interlocutore;
Utilizzare filtri, software che impediscono il collegamento ai siti web per adulti (black list);
Le azioni di contenimento degli incidenti previste sono le seguenti:
Se l'alunno viene infastidito od offeso, suggerire di modificare i dettagli della privacy del proprio profilo, in modo tale che solo gli utenti autorizzati siano in grado di

vederlo (MSN messengers, siti social network,Skype etc.), o suggerirgli di bloccare particolari mittenti.
Consigliare di cambiare il proprio indirizzo e-mail o, se necessario, cambiare il numero di cellulare contattando l'operatore telefonico;
Fare cancellare il materiale offensivo dal telefonino, facendo intervenire i genitori;
Contattare la polizia se si ritiene che il materiale offensivo sia illegale. In caso di foto e video pedopornografici, confiscare il telefonino o altri dispositivi ed evitare di eseguire download, produrne copie, condividerne link o postarne il contenuto, poiché ciò è reato per chiunque.
Vengono inoltre delineate le azioni da eseguire qualora un utente minorenne o maggiorenne accidentalmente accede a un sito web che contiene materiale illegale:
-allontanarsi immediatamente dal sito
-parlarne con un adulto (se ad accedervi è un minore)
-segnalare il sito alla polizia postale attraverso il link: https://www.commissariatodips.it/collabora.html.
Al sito della polizia postale tra l'altro possono anche essere inviate altri tipi di segnalazioni di qualunque attività fraudolenta on-line.

Rilevazione

Che cosa segnalare

Gli alunni possono mostrare segni di tristezza o di ansia o di risentimento nei confronti di compagni o di altri e riferire l'accaduto spontaneamente o su richiesta ai docenti. I fatti riferiti possono essere accaduti anche al di fuori della scuola. Anche confrontandosi periodicamente con gli alunni sui rischi delle comunicazioni on-line, i minori possono riferire di fatti o eventi personali o altrui che "allertano" l'insegnante.
Mentre il docente è autorizzato a controllare le strumentazioni della scuola, per controllare l'uso del telefono cellulare di un alunno si rivolge al genitore.
I contenuti "pericolosi" comunicati/ricevuti a/da altri, messi/scaricati in rete, ovvero le tracce che possono comprovare l'utilizzo incauto, scorretto o criminoso degli strumenti digitali utilizzabili anche a scuola dai minori possono essere i seguenti:
-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, ecc.);
-Contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);
-Contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte (pedopornografia), ecc.

Come segnalare: quali strumenti e a chi.

Gli insegnanti, anche con l'ausilio dell'Animatore digitale, possono provvedere a conservare le prove della condotta incauta o scorretta rilevate sui pc della scuola: soprattutto la data e l'ora, il contenuto dei messaggi e, se possibile, l'ID del mittente (es. username, mail, numero di telefono cellulare) o l'indirizzo web del profilo ed il suo contenuto.

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

Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno, quantunque riferite a fatti accaduti anche 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.

In particolare la segnalazione viene fatta a entrambe le famiglie, se oltre alla vittima anche l'autore della condotta negativa è un altro alunno.

Per le segnalazioni di fatti rilevati sono previsti i seguenti strumenti che i docenti possono utilizzare sulla base della gravità dell'accaduto:

-Annotazione del comportamento sul registro e comunicazione scritta ai genitori, che la devono restituire vistata;

-Convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti;

-Relazione scritta al Dirigente scolastico.

In base all'urgenza le comunicazioni formali possono essere precedute da quelle informali, effettuate per le vie brevi.

Inoltre per i reati meno gravi la legge rimette ai genitori degli alunni la scelta di richiedere la punizione del colpevole, attraverso la querela.

Per i reati più gravi gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti).

In particolare per i fatti criminosi, ai fini della denuncia, la relazione deve essere redatta nel modo più accurato possibile, indicando i seguenti elementi: il fatto, il giorno dell'acquisizione del fatto nonché le fonti di prova già note e per quanto possibile, le generalità, il domicilio e quant'altro di utile a identificare la persona alla quale il reato è attribuito, la persona offesa, e tutti coloro che sono in grado di riferire circostanze rilevanti per la ricostruzione del fatto.