ISTITUTO COMPRENSIVO STATALE "FERRUCCI"
Via Puccini, 196 - 51036 LARCIANO (PT)
Tel. 0573838334 Fax. 057383020 - Codice Fiscale: 80007970470
Codice Meccanografico: PTIC81300L
Email ptic81300l@istruzione.it ptic81300l

E-Safety Policy

Introduzione

- Scopo della Policy

Il presente documento ha lo scopo di illustrare all'utenza le regole per un uso corretto e responsabile degli strumenti tecnologici e della rete in uso nell'Istituto.

L'Istituto intende promuovere lo sviluppo della competenza digitale, che passa attraverso la conoscenza di procedure e competenze tecniche e di norme comportamentali, dettate da un uso consapevole e critico da parte degli alunni, delle tecnologie digitali e di internet. Lo scopo è, dunque, prevenire e eventualmente rilevare e affrontare, situazioni derivanti da un uso pericoloso delle stesse.

Il primo passo è informare gli alunni dei rischi cui si espongono nella navigazione in rete, mentre dal canto suo l'Istituto si attiva per limitare l'accesso a siti potenzialmente dannosi, i cui contenuti possano risultare illegali o inadeguati. Gli insegnanti, infine, hanno il ruolo di guidare le attività on-line a scuola e illustrare le regole di comportamento per la navigazione in rete anche a casa.

Ai docenti, in particolare, spetta il ruolo di informare, piuttosto che censurare, gli alunni affinché imparino ad usare consapevolmente i contenuti e i servizi della rete per conoscere gli effetti cognitivi, comportamentali delle sue potenzialità oltre alle informazioni utili a gestire gli strumenti tecnologici.

Di seguito si schematizzano i rischi cui la comunità scolastica è sottoposta.

Rischi per gli utenti

- valutazione di autenticità ed esattezza dei contenuti on-line bullismo on-line
- sexting
- grooming
- violazione della privacy
- salute
- copyright

Ruoli e Responsabilità (che cosa ci si aspetta da tutti gli attori della comunità scolastica)

1. Dirigente Scolastico

E' garante:

- dei dati e della sicurezza dei dati
- di un accesso protetto e filtrato della rete internet
- formazione del personale sull'uso delle tecnologie informatiche delle procedure da attuare in caso d'infrazione della e-policy
- dell'esistenza di un sistema di monitoraggio interno periodico della sicurezza on-line

2. DSGA

Si impegna a:

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

scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet

3. L'Animatore Digitale ed il suo team, il referente per bullismo e cyberbullismo e la Funzione strumentale dell'Area Informatica (su nomina del D.S.)

Si impegnano a:

- stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on line e alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- assicurare che tutto il personale sia a conoscenza delle procedure da seguire per la segnalazione e la gestione in caso d'infrazione della sicurezza on line
- assicurare che tutto il personale sia a conoscenza delle procedure da seguire in caso di segnalazione e gestione di casi di cyberbullismo, in tutte le sue forme
- coordinare i contatti con le autorità locali e le autorità competenti
- monitorare e relazionano al D.S. periodicamente circa la sicurezza on line
- diffondere la conoscenza della e-safety presso la comunità scolastica
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".

4.I docenti

Si impegnano a:

- informarsi/aggiornarsi sulle tematiche relative alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e di rispettare il presente regolamento integrare le suddette tematiche nel curriculo scolastico
- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore
- garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- 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
- controllare l'accesso a internet e l'uso delle tecnologie digitali e dei dispositivi mobili da parte degli alunni, durante le attività scolastiche (ove consentito)
- segnalare al D.S. qualsiasi difficoltà, bisogno o abuso da parte degli alunni, nell'utilizzo delle tecnologie digitali
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo alla Funzione strumentale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC

5. Il personale ATA

Il personale ATA:

- comprende e contribuisce a promuovere la politica di e-safety della scuola
- segnala eventuali abusi nell'uso delle tecnologie digitali e di accesso a internet

6. Gli alunni

Si impegnano a:

- leggere, comprendere e rispettare il documento di e-safety
- rispettare le norme sul diritto d'autore, nell'utilizzo consapevole delle grandi possibilità di ricerca offerte dalla rete, evitando il plagio
- capire l'importanza di segnalare abusi e condotte non adeguate rispetto ai contenuti on line
- utilizzare le tecnologie digitali e i dispositivi mobili se autorizzati dai docenti
- comprendere l'importanza di adottare buone pratiche di sicurezzza on-line quando si utilizzano le tecnologie digitali per non correre rischi
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori
- adottare comportamenti rispettosi degli altri anche nella comunicazione in rete

7. I genitori

Si impegnano a:

- sostenere la politica di salvaguardia di sicurezza on line della scuola
- leggere e comprendere l'importanza dell'accordo di e-policy con la scuola
- seguire i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti anche nello studio a casa, controllando in particolare l'utilizzo del pc e di internet
- partecipare alle iniziative proposte dalla scuola sul tema

Condividere e la Policy all'interno dell'intera comunità scolastica.

a) 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 potranno essere utilizzati solo con l'autorizzazione degli insegnanti
- Uno o più moduli di insegnamento sulla e-safety saranno programmati nell'arco dell'anno per aumentare la consapevolezza e importanza di un uso sicuro e responsabile di internet tra gli alunni.
- L'istruzione degli alunni riguardo all'uso responsabile e sicuro di internet precederà l'accesso alla rete.
- 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.

b) 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 (consigli di interclasse/intersezione, collegio dei docenti) e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web.
- 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 e dalla Funzione strumentale dell'area informatica, che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici.

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

c) Condividere e comunicare la politica di e-safety ai genitori

- L'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di internet sarà attirata nelle news o in altre aree del sito web della scuola.
- Sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali.
- La funzione strumentale dell'area informatica e l'Animatore digitale forniranno ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di internet anche a casa.
- L'Animatore digitale, la funzione strumentale dell'area informatica e i docenti di classe forniranno ai genitori indirizzi sul web relativi a risorse utili per lo studio e a siti idonei ed educativi per gli alunni
- I genitori esperti potranno collaborare nelle attività di informazione/formazione del personale e degli alunni.

Gestione delle infrazioni alla Policy.

1) Disciplina degli alunni

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 della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare
- l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono
- la comunicazione incauta e senza permesso con sconosciuti
- il collegamento a siti web non indicati dai docenti
- un uso offensivo e lesivo della dignità propria e altrui della comunicazione in rete
- comportamenti connessi a sexting (invio di testi o immagini sessualmente esplicite tramite Internet o telefono cellulare) e sextorsion (richiesta di denaro per non pubblicare foto o video sessualmente esplicite ritraenti la vittima), cyberstalking (molestare una vittima mediante comunicazione elettronica, tramite e-mail o messaggi diretti), istigazione al suicidio, detenzione e diffusione di materiale pedopornografico, impersonation (furto d'identità), fake identity (identità contraffatta), baiting (attività che mira a creare contenuti web per attrarre ("pescare") quanti più utenti possibili in modo da presentare loro contenuti pubblicitari), cyberbulling (Atto aggressivo, prevaricante o molesto compiuto tramite strumenti telematici).
- l'utilizzo delle tecnologie informatiche e dei dispositivi mobili non autorizzati dal docente
- l'accesso a siti internet non autorizzati dal docente

Per prima cosa dovrà essere effettuata la segnalazione al referente bullismo/cyberbullismo e alla FS Area Informatica che relazioneranno al D.S. che valuterà il coinvolgimento delle famiglie e delle autorità preposte.

Le sanzioni includeranno

- richiamo verbale
- richiamo scritto
- la convocazione dei genitori da parte del coordinatore di classe e del referente
- la convocazione dei genitori da parte del Dirigente scolastico

2) Disciplina del personale scolastico

Le possibili infrazioni del personale docente sono così di seguito schematizzate:

- utilizzo delle tecnologie della scuola, ivi compresa la rete WI FI dell'Istituto non connesso alle attività d'insegnamento o al profilo professionale
- utilizzo delle comunicazioni elettroniche con alunni e genitori non compatibile con il ruolo professionale
- violazione della privacy nel trattamento dei dati personali degli alunni
- diffusione delle password
- mancata informazione degli alunni sul corretto e responsabile uso di tecnologie e strumenti informatici e di internet
- mancata vigilanza nell'utilizzo degli stessi
- mancata segnalazione di situazioni critiche rispetto alla e-policy d'istituto

Le procedure di sanzione sono quelle previste dalla legge e dai contratti di lavoro.
Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone una copia per eventuali successive investigazioni.
Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo-gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

3) Disciplina dei genitori

In considerazione dell'età degli alunni e della loro dipendenza dagli adulti, alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico. Le situazioni familiari meno favorevoli sono:

- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai
- una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone
- un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei
- un utilizzo del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria indirizzi o contenuti non idonei.

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

Monitoraggio dell'implementazione della Policy e suo aggiornamento.

Il referente bullismo/cyberbullismo e la FS Area Informatica, in accordo con l'Animatore Digitale e sotto la supervisione del D.S. si occuperanno di rivedere ogni anno il documento di e-policy consultando l'apposita commissione. La revisione sarà registrata e approvata dal Collegio Docenti.

Integrazione della Policy con Regolamenti esistenti.

La policy richiede l'integrazione con il Regolamento d'Istituto e regolamenti allegati:

Allegato A del Regolamento d'Istituto "**REGOLAMENTO PER L'USO DELLE TIC"**
Art. 68 comma 2 del Regolamento d'Istituto

Formazione e Curricolo

Curricolo sulle competenze digitali per gli studenti.

Inserita nelle otto Competenze chiave di cittadinanza attiva indicate dal Consiglio di Lisbona nel marzo 2000, la competenza digitale viene così definita all'interno della "Raccomandazione del Parlamento europeo e del Consiglio" del 18 dicembre 2006, relativa a competenze chiave per l'apprendimento permanente (2006/962/CE):
"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 2012 come ben esplicitato dall'autrice Franca Da Re (Dal Curricolo Scuola Primaria e Secondaria di I grado di Franca Da Re – Indicazioni Nazionali 2012):
<<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. L'Istituto si propone di integrare il curricolo scolastico degli studenti con attività educative che favoriscano la cultura della sicurezza on line.
In tal senso si impegna a sviluppare una serie di competenze e comportamenti adeguati alle età degli alunni, tra cui:

- programmare attività e far partecipare gli alunni a laboratori di Coding in occasione della Settimana del codice;
- sviluppare una serie di strategie per valutare e verificare le informazioni prima di accettare l'esattezza, sviluppando il pensiero critico;
- sapere come restringere o affinare una ricerca; utilizzare software per la presentazione di dati; sviluppare la cultura del "software libero";
- assumere comportamenti adeguati in ambienti on line, rispettosi della dignità propria e altrui;

- essere consapevoli che dati personali e fotografie possono essere manipolate e usate in maniera fraudolenta e lesiva da parte di terzi;
- comprendere che le "identità virtuali" possono essere ingannatorie;
- capire il motivo per cui non devono pubblicare foto o video di altri senza il loro permesso;
- conoscere le norme in materia di copyright;
- sviluppare una sempre maggiore sensibilità verso l'impatto che il cyberbullismoe le altre forme dì prevaricazione possono avere sulla vita propria e dei compagni e sapere a chi rivolgersi per segnalare abusi connessi all'utilizzo di internet;
- utilizzare con attenzione Internet per garantire che si adatti alla loro età e sia di sostegno agli obiettivi di apprendimento per le aree curriculari specifiche.

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

In attuazione del PNSD questo Istituto ha realizzato:

- individuazione e formazione di un Animatore Digitale;
- formazione dei docenti all'utilizzo del registro elettronico e dello scrutinio elettronico;
- somministrazione di un questionario rivolto ai docenti per la rivelazione dei bisogni "digitali";
- realizzazione/ampliamento della rete WI-FI/LAN dei tre plessi dell'Istituto;
- ricognizione e messa a punto delle dotazioni digitali;
- attivazione e comunicazione di iniziative di formazione, in particolare rivolte allo sviluppo e alla diffusione del Coding e del pensiero computazionale;
- coinvolgimento delle famiglie nella stesura della e-policy d'istituto, attraverso i consigli di intersezione e di classe.

La scuola ha inoltre previsto la diffusione di iniziative rivolte a:

- monitoraggio del piano digitale di Istituto e dei risultati conseguiti;
- formazione a disposizione del personale in materia di sicurezza on-line attraverso corsi di formazione e/o aggiornamento;
- una politica di informazione e diffusione della e-safety d'Istituto**;**

Sensibilizzazione delle famiglie.

L' Istituto s'impegna a promuovere una cultura dell'informazione, volta a coinvolgere le famiglie nella cultura di un uso consapevole delle tecnologie digitali e di internet, attraverso:

- una conoscenza e condivisione del Regolamento della Policy, al fine di garantire che i principi di comportamento sicuro on-line siano chiari;
- un'informazione attraverso il sito della scuola;
- incontri di consulenza con esperti;
- fornire informazioni sui siti nazionali di sostegno per i genitori, quali il sito www.generazioniconnesse.it.

Gestione dell'infrastruttura e della strumentazione ICT della scuola.

Accesso ad internet: filtri antivirus e sulla navigazione, gestione accessi (password, backup, ecc.)

Sito web
Tutte le iniziative didattiche, 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.

Sicurezza Rete LAN/WLAN

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 dispositivi alla rete di Istituto deve essere autorizzato dal Dirigente Scolastico e di una rete WLAN il cui accesso è autorizzato ai docenti dal D.S., tramite password.
La rete interna è protetta da Firewall per quanto riguarda le connessioni con l'esterno. Le postazioni sono protette con sistemi antivirus.

Sito web della scuola
La scuola attualmente ha un sito web. Tutti i contenuti del settore didattico sono pubblicati direttamente e sotto supervisione dell'Animatore digitale e della Funzione Strumentale dell'Area informatica, 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.

Protezione dei dati personali.
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.

Strumentazione personale

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

In attuazione del PNSD che prevede un sempre maggiore coinvolgimento delle tecnologie digitali nelle attività curriculari, agli studenti è consentito l'utilizzo del cellulare e del tablet, solo se autorizzato da un docente per ragioni esclusivamente didattiche.

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

I docenti e il personale della scuola possono utilizzare cellulari e altri dispositivi a scopo personale non durante l'attività didattica o lavorativa. Possono usufruire della connessione WIFI dell'Istituto, anche su proprio dispositivo, solo ed esclusivamente a scopo didattico.

5. Prevenzione, rilevazione e gestione dei casi

Prevenzione

- Rischi

I rischi cui un allievo può incorrere a scuola nell'utilizzo delle TIC derivano da un uso dello smartphone, dei pc della scuola collegati alla rete e dei tablet. Eludendo la sorveglianza degli insegnanti, gli allievi potrebbero incorrere in tutti i rischi connessi all'uso non corretto di 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, anche attraverso attività mirate alla conoscenza del fenomeno del cyberbullismo;
- creare degli spazi in cui gli alunni si possano confrontare su questo tema, utilizzando come spunti di riflessione: spezzoni di film, canzoni, materiali prodotti da altri alunni coinvolti nel progetto SIC;
- confrontarsi con gli altri insegnanti della classe, della scuola o con esperti del territorio; rivolgersi alla helpline di generazioni connesse (www.generazioniconnesse.it).;
- 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)
- consentire l'utilizzo del cellulare solo per scopi didattici e sotto il controllo dei docenti;

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 spontaneamente o su richiesta l'accaduto ai docenti. I fatti riferiti possono essere accaduti anche al di fuori della scuola. Nel momento in cui un docente viene a conoscenza di fatti, avvenuti anche fuori dalla scuola, è tenuto a segnalare quanto saputo nelle modalità di seguito descritte.
I contenuti "pericolosi" per gli alunni possono essere i seguenti:

- contenuti che violino la 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 discriminatori che inneggiano al suicidio, immagini o video umilianti, insulti, ecc.)
- contenuti che implichino la sfera della sessualità

Come segnalare: quali strumenti e a chi.

- Rilevazione e gestione dei casi

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

1. Annotazione del comportamento sul registro e comunicazione scritta ai genitori, che la devono restituire vistata.
2. Convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti.
3. Relazione scritta al Dirigente scolastico.

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.

Gestione dei casi

Definizione delle azioni da intraprendere a seconda della specifica del caso

Gestione dei casi di "immaturità"

Può sembrare naturale all'alunno fornire i propri dati sui siti allestiti in modo tale da attrarre l'attenzione degli adolescenti, con giochi e animazioni, personaggi simpatici e divertenti, che richiedono una procedura di registrazione.

Curiosità, manifestazioni di reciproco interesse tra pari, idee e fantasie sulla sessualità sono espressione da una parte del progressivo sviluppo socio-affettivo dell'alunno e dall'altra dei molteplici messaggi espliciti che gli giungono quotidianamente attraverso i media (televisione, DVD, internet, giornali e riviste), i discorsi degli altri alunni o degli adulti.

I comportamenti cosiddetti "quasi aggressivi", che spesso si verificano tra coetanei, le interazioni animate o i contrasti verbali, o la presa in giro "per gioco", effettuata anche in rete, mettono alla prova la relazione con i compagni, la supremazia o la parità tra i soggetti implicati e l'alternanza e sperimentazione dei diversi ruoli. Il gruppo dei pari rappresenta anche il momento di conquista dell'autonomia dall'adulto e pertanto luogo di "complicità" e di piccole "trasgressioni", di scambi "confidenziali" condivisi fra gli amici nella rete o con il cellulare.

Detti comportamenti, che finiscono per arrivare all'attenzione degli adulti, sono controllati e contenuti dai docenti attraverso i normali interventi educativi, di richiamo al rispetto delle regole di convivenza civile e democratica, di rispetto degli altri, per evitare che possano degenerare, diventare pericolosi per sé o offensivi e minacciosi per gli altri.

Gestione dei casi di "prepotenza" o "prevaricazione"

I comportamenti definibili "cyberbullismo" possono esprimersi nelle forme più varie e non sono tratteggiabili a priori, se non contestualizzandoli. Le caratteristiche che aiutano a individuarli e a distinguerli dallo scherzo, dalle intemperanze caratteriali, dai diverbi usuali

fra i ragazzi sono la costanza nel tempo e la ripetitività, l' asimmetria (disuguaglianza di forza e di potere), il disagio della/e vittima/e.
Il cyberbullismo si esplica infatti con comportamenti e atteggiamenti costanti e ripetitivi di arroganza, prepotenza, prevaricazione, disprezzo, dileggio, emarginazione, esclusione ai danni di una o più persone, agiti da un solo soggetto, ma in genere da un gruppo.
Nel caso particolare del Cyberbullismo le molestie sono attuate attraverso strumenti tecnologici:
•invio di sms,messaggi in chat, e-mail offensive o di minaccia;
• diffusione di messaggi offensivi ai danni della vittima, attraverso la divulgazione di sms o e-mail nelle mailing-list o nelle chat-line;
• pubblicazione nel cyberspazio di foto o filmati che ritraggono prepotenze o in cui la vittima viene denigrata. Il cyberbullismo in particolare può originarsi anche dall'esasperazione di conflitti presenti nel contesto scolastico. Il conflitto, presente in ogni normale interazione, è da considerarsi come un campanello d'allarme e può degenerare in forme patologiche quando non lo si riconosce e gestisce in un'ottica evolutiva dei rapporti, di negoziazione e risoluzione. Se non gestito positivamente, infatti, il conflitto rischia di mutarsi e provocare effetti distruttivi sulle relazioni (prevaricazione e sofferenza) e sull'ambiente (alterazione del clima del gruppo-classe).
In considerazione dell'età degli alunni possono prefigurarsi alcune forme di interazioni che possono evolvere verso tale fenomeno. Per prevenire e affrontare il cyberbullismo dunque i docenti non solo identificano vittime e prepotenti in divenire, ma tutti insieme affrontano e intervengono sul gruppo-classe, coinvolgendo i genitori degli allievi.
L'elemento fondamentale per una buona riuscita dell'intervento educativo è infatti la corretta, compiuta e convinta ristrutturazione dell'ambiente sociale in cui tale fenomeno si verifica, e in particolare delle relazioni nel contesto della classe. Gli atteggiamenti degli alunni, così come quelli dei loro genitori, possono giocare un molto significativo nel ridurre la dimensione del fenomeno.
Gli interventi mirati sul gruppo classe sono gestiti dal referente in collaborazione con il team dei docenti della classe e d'intesa con le famiglie - ad esempio con percorsi di mediazione volta alla gestione positiva del conflitto, con gruppi di discussione (circle time), con rappresentazioni e attività di role-play sull'argomento del cyberbullismo, con le strategie del problem solving.
Vengono intrapresi anche i percorsi individualizzati di sostegno alle vittime, volti a incrementarne l'autostima e l'assertività e a potenziare le risorse di interazione sociale, mentre i prevaricatori sono destinatari di interventi mirati a smuoverne le competenze empatiche e a favorire una loro condivisione delle norme morali.
Anche in relazione alle manifestazioni socio-affettive fra pari, al linguaggio sessualizzato o "volgare", al fine di evitare prevaricazioni e imbarazzo o disagio, i docenti intervengono per favorire negli alunni un buon rapporto con il proprio corpo e per far percepire meglio eventuali violazioni dei limiti di prossimità o di "confidenza" ed imparare ad opporvisi, per far acquisire fiducia nelle proprie sensazioni e nel proprio intuito e determinazione nel rifiutare i contatti anche "a distanza" sgradevoli o "strani", per rendere consapevoli gli alunni del diritto al rispetto dei propri limiti e di quelli altrui, per far capire ai ragazzi che l'interazione on-line deve sottostare a delle regole di buon comportamento, né più né meno della comunicazione a viso aperto, quale quella della vita reale.
Inoltre la scuola, qualora rilevi una situazione psico-socio-educativa particolarmente problematica, convoca i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi. Consiglia altresì di servirsi dello sportello di ascolto psicologico gratuito se attivo presso la scuola. Promuove e supporta la richiesta delle famiglie rivolta ai Servizi Sociali dell'Ente Locale per la fruizione di servizi socio-educativi

comunali e alla ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare).

Gestione degli "abusi sessuali"

Lo spettro delle forme di abuso e di violenza è diventato ancora più ampio e subdolo in seguito alle possibilità offerte dai nuovi mezzi di comunicazione come internet, il cellulare o altri dispositivi tecnologici, e il loro utilizzo sempre più diffuso non fa che acuire il problema. Internet, infatti, permette di scaricare o vendere immagini o filmati di pornografia infantile.

Succede sempre più frequentemente che un adulto prenda contatto con dei bambini nei forum o nelle chat su internet, e che li metta di fronte a domande o messaggi sessuali o addirittura a immagini pornografiche. A volte l'adulto induce i bambini a spogliarsi davanti alla webcam oppure a inviare una fotografia che li ritrae nudi tramite internet o sul cellulare, per poi ricattarli e costringerli a non rivelare gli abusi. Spesso l'adulto finge di essere minorenne.

La denuncia all'autorità giudiziaria o agli organi di Polizia, da parte degli insegnanti o del Dirigente scolastico, costituisce il passo necessario per avviare un intervento di tutela a favore della vittima e attivare un procedimento penale nei confronti del presunto colpevole.

La presa in carico di situazioni di abuso sessuale, così delicate e complesse, richiede un approccio multidisciplinare, da parte di diverse figure professionali. I versanti su cui si articola l'intervento possono essere essenzialmente tre: medico, socio-psicologico e giudiziario.

Il compito della scuola non è comunque solo quello di "segnalare", ma più ampio ed importante, soprattutto nella prevenzione dell'abuso, nonché nella ripresa della piccola vittima, in quanto ha al suo interno fattori relazionali ed educativi che possono aiutare il bambino a riprendere una crescita serena.

A tal fine la scuola lavora insieme alle altre figure professionali e alle famiglie, scambiando informazioni e condividendo progetti e prassi operative, favorendo le occasioni di confronto e di dialogo.

La commissione

Referenti bullismo e cyberbullismo
Ivana Gamenoni (Scuola Primaria) Serena Innocenti (Scuola Secondaria di Primo Grado)
Vicaria del Dirigente Scolastico
Prof.ssa Daniela Calugi
Rappresentanti dei genitori
Marzia Gavazzi (Scuola Primaria) Manila Maccioni e Ilaria Meacci (Scuola Secondaria di Primo Grado)
Rappresentante personale ATA
Carmela Ruggiero
Rappresentanti degli alunni
Christian Gammuto e Angela Giambrone (Presidente e Vicepresidente Teencoop a.s. 2017/2018)
Ludovica Fagni e Filippo Parlanti (Sindaco e Vice sindaco del Consiglio Comunale dei Ragazzi)

1. Procedure operative per la gestione delle infrazioni alla Policy.

MODULO DI RICHIESTA DI CREDENZIALI DI AUTENTICAZIONE/DI ACCESSO AD INTERNET NELLA RETE DI ISTITUTO E DI UTILIZZO DEI DISPOSITIVI ELETTRONICI

Al Dirigente Scolastico
I.C. "F. Ferrucci"
Larciano (PT)

Il/La sottoscritto/a _____, nato/a a _____ (___), il _____, residente a _____ in via _____, n. _____ CAP _____ email _____ in qualità di **docente/personale ATA** (cancellare la voce che non interessa) in servizio presso l'I.C. "F. Ferrucci":
chiede il rilascio delle credenziali di autenticazione /l'accesso ad Internet nella rete di Istituto.
Dichiara
- di aver letto e compreso il documento di "Policy e-safety", di utilizzo accettabile della rete internet, pubblicato sul sito della Scuola;
- di essere consapevole delle implicazioni di responsabilità personale derivanti dall'accesso alla rete internet e dagli eventuali abusi.
In particolare si impegna a:
- non scaricare/duplicare/distribuire software o altri contenuti protetti da diritto d'autore;
- non accedere a siti o risorse dal contenuto illegale o non consono alle regole di comportamento dettate dal carattere istituzionale ed educativo della scuola (ad esempio, siti con contenuto violento, pedo-pornografico, razzista, etc…);
- non collegarsi ad internet a scopi commerciali o di profitto personale e per attività illegali;
- non diffondere virus o altri software malevoli all'interno della rete e a dare immediato avviso all'Amministrazione della Rete di comportamenti anomali o di infezioni riconosciute;
- conservare le credenziali di accesso alla rete in modo scrupoloso, non comunicandole ad altre persone. E' consapevole che l'accesso attraverso l'autenticazione trasferisce direttamente la responsabilità degli atti commessi durante la navigazione all'intestatario delle credenziali stesse.
Dichiara di essere consapevole che:
-l'autorizzazione all'uso della rete di Istituto potrà venire revocata (cancellazione dell'utente) in qualsiasi momento per cause tecniche o per motivazioni legate all'uso improprio o alla violazione delle norme di comportamento;
-l'utilizzo dei dispositivi elettronici e della rete della scuola deve essere utilizzata per attività di servizio o funzionali alle stesse;
- l'utilizzo della rete per l'assunzione di impegni o responsabilità per conto della scuola deve essere autorizzata dal dirigente scolastico, legale rappresentante dell'istituzione nonché legittimo titolare dell'utenza
- l'utilizzo del cellulare e di altri dispositivi elettronici personali a scuola deve avvenire nei limiti consentiti dalla legge e dai regolamenti dell'istituzione scolastica, in situazioni di necessità ed urgenza o per ragioni di servizio;
- ci si deve rivolgere per la necessaria assistenza alla connessione o al funzionamento dei dispositivi contattando l'Animatore digitale o il referente del laboratorio di informatica o gli uffici di segreteria, evitando tentativi incerti di ripristino o di modificazione delle impostazioni.

Data _____ Firma leggibile _____

Procedure operative per la gestione dei casi.

LINEE GUIDA PER ALUNNI

- Non comunicare mai a nessuno la tua password e periodicamente cambiala, usando numeri, lettere e caratteri speciali
- Mantieni segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della tua scuola.
- Non inviare a nessuno fotografie tue o di tuoi amici.
- Prima di inviare o pubblicare la fotografia di qualcuno, chiedi sempre il permesso scritto: se la persona ritratta nella fotografia è minorenne ci vuole il consenso scritto dei genitori
- Chiedi sempre al tuo insegnante a scuola o ai tuoi genitori a casa il permesso di scaricare documenti da Internet.
- Chiedi sempre il permesso prima di iscriverti a qualche concorso o prima di riferire l'indirizzo della tua scuola.
- Quando sei connesso alla rete RISPETTA SEMPRE GLI ALTRI: ciò che per te è un gioco può rivelarsi offensivo per qualcun altro.
- Non rispondere alle offese ed agli insulti.
- Conserva le comunicazioni offensive, ti potrebbero essere utili per dimostrare quanto ti è accaduto.
- Se ricevi materiale offensivo (email, sms, mms, video, foto, messaggi vocali) non diffonderlo: potresti essere accusato di cyberbullismo.
- Rifletti prima di inviare: ricordati che tutto ciò che invii su internet diviene pubblico e rimane per SEMPRE.
- 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.
- Se qualcuno su Internet ti chiede un incontro di persona, riferiscilo al tuo insegnante o ai tuoi genitori.
- Ricordati che le persone che incontri nella Rete sono degli estranei e non sempre sono quello che dicono di essere.
- Non caricare (upload) materiale video o fotografico nei siti web dedicati senza il permesso del tuo insegnante o dei tuoi genitori.

LINEE GUIDA PER INSEGNANTI

- Evitate di lasciare le e-mail o file personali aperti sui computer.
- Salvate sempre i vostri lavori (file) sulla cartella personale presente nell'area di condivisione.
- Discutete con gli alunni della policy e-safety della scuola, di utilizzo consentito della rete, e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di Internet.
- Date chiare indicazioni su come si utilizza Internet, ed eventualmente anche la posta elettronica, e informateli che le navigazioni saranno monitorate.
- Ricordate di chiudere la connessione (e di spegnere il computer) alla fine della sessione di lavoro su Internet e disabilitare la navigazione su Internet del laboratorio (qualora sia stata attivata).
- Ricordate agli alunni che la violazione consapevole della policy e-safety della scuola, di utilizzo consentito della rete, comporta sanzioni di diverso tipo.
- Adottate provvedimenti "disciplinari", proporzionati all'età e alla gravità del comportamento.
- Adottate interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni.
- Nelle situazioni psico-socio-educative particolarmente problematiche, convocate i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi (sportello di ascolto psicologico gratuito attualmente attivo presso la scuola, Servizi Sociali per la fruizione di servizi socio-educativi comunali, ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare).
- Segnalate la presenza di materiale pedopornografico (senza scaricarlo o riprodurlo) alla Polizia Postale o al Telefono Azzurro.
- In caso di abuso sessuale rilevato anche attraverso i nuovi mezzi di comunicazione come internet o il cellulare, confrontatevi con i colleghi di classe e il Dirigente Scolastico, denunciate all'autorità giudiziaria o agli organi di Polizia.

CONSIGLI AI GENITORI PER UN USO RESPONSABILE DI INTERNET A CASA
1) Consigli generali

- Posizionate il computer in una stanza accessibile a tutta la famiglia.
- Evitate di lasciare le e-mail o file personali sui computer di uso comune.
- Concordate con vostro figlio le regole: quando si può usare internet e per quanto tempo.
- Inserite nel computer i filtri di protezione: prevenite lo spam, i pop-up pubblicitari, l'accesso a siti pornografici.
- Aumentate il filtro del "parental controll" attraverso la sezione sicurezza in internet dal pannello di controllo.
- Attivate il firewall (protezione contro malware) e antivirus.
- Mostratevi coinvolti: chiedete a vostro figlio di mostrarvi come funziona internet e come viene usato per scaricare e caricare compiti, lezioni, materiali didattici e per comunicare con l'insegnante.
- Incoraggiate le attività on line di alta qualità: ricercare informazioni scientifiche, ricercare nuovi amici nel mondo.
- Partecipate alle esperienze on line: navigate insieme a vostro figlio, incontrate amici on line, discutete gli eventuali problemi che si presentano.
- Comunicate elettronicamente con vostro figlio: inviate, frequentemente, E-mail, InstantMessage.
- Spiegate a vostro figlio che la password per accedere ad alcune piattaforme è strettamente personale e non deve essere mai fornita ai compagni o ad altre persone.
- Stabilite ciò che ritenete inaccettabile (razzismo, violenza, linguaggio volgare, pornografia).
- Discutete sul tema dello scaricare file e della possibilità di ricevere file con virus.
- Raccomandate di non scaricare file da siti sconosciuti.
- Incoraggiate vostro figlio a dirvi se vedono immagini particolari o se ricevono e-mail indesiderate.
- Discutete nei dettagli le conseguenze che potranno esserci se vostro figlio visita deliberatamente siti non adatti, ma non rimproveratelo se compie azioni involontarie.
- Spiegate a vostro figlio che le password, i codici pin, i numeri di carta di credito e i numeri di telefono e i dettagli degli indirizzi e-mail sono privati e non devono essere dati ad alcuno.
- Spiegate a vostro figlio che non tutti in Internet sono chi realmente dichiarano di essere; di conseguenza i vostri ragazzi non dovrebbero mai accordarsi per appuntamenti senza consultarvi prima.
- Il modo migliore per proteggere vostro figlio è usare Internet con loro, discutere e riconoscere insieme i rischi potenziali.