Ministero dell'Istruzione, dell'Università e della Ricerca
ISTITUTO COMPRENSIVO CASTELVERDE
ISTITUTO COMPRENSIVO CASTELVERDE – Via Massa di San Giuliano, 131 – 00132 ROMA
CODICE MECCANOGRAFICO: RMIC8CP00E CODICE FISCALE: 97616500589
Tel: 06 455 90 500 E-mail: rmic8cp00e@istruzione.it –
rmic8cp00e@pec.istruzione.it***www.iccastelverderoma.edu.it***

1. introduzione

Scopo della Policy.

Lo scopo della E-Safety Policy è quello di informare l'utenza per un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente.

In particolare l'intento della scuola è quello di promuovere l'uso consapevole e critico da parte degli alunni delle tecnologie digitali e di internet, di far acquisire loro procedure e competenze "tecniche" ma anche corrette norme comportamentali, di prevenire ovvero rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali. Gli utenti, siano essi maggiorenni o minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto la Scuola promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti. In questo contesto, gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose.

Le principali aree di rischio per la nostra comunità scolastica possono essere riassunte come segue:

Contenuto

- l'esposizione a contenuti inappropriati
- visita di siti web inappropriati
- siti di odio
- validazione dei contenuti: come controllare l'autenticità e l'esattezza dei contenuti online.

Contatto

- grooming
- bullismo on-line in tutte le forme
- il furto di identità.

Condotta

- questioni di privacy, tra cui la divulgazione di informazioni personali
- reputazione online
- la salute e il benessere (quantità di tempo speso online su Internet o giochi)
- sexting (invio e ricezione di immagini personali intime)
- l'estremismo
- Copyright (poca cura o considerazione per i diritti d'autore relativamente a musica e film).

Ruoli e Responsabilità (che cosa ci si aspetta da tutti gli attori della Comunità Scolastica).

RUOLO	RESPONSABILITÀ
Il Dirigente Scolastico	● la responsabilità generale per i dati e la sicurezza dei dati; ● la responsabilità di assicurare che il personale riceva una formazione adeguata per svolgere i ruoli di sicurezza online e per la formazione di altri colleghi; ● essere a conoscenza delle procedure da seguire in caso di infrazione della E-Safety Policy; ● ruolo di primo piano nello stabilire e rivedere la E-Safety Policy; ● ricevere relazioni di monitoraggio periodiche della sicurezza online da parte del responsabile;
I responsabili della sicurezza online (DSGA, docente su nomina del DS e docente referente per il cyberbullismo)	● La responsabilità per i problemi di sicurezza online; ● promuovere la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica; ● assicurare che l'educazione alla sicurezza online sia incorporata in tutto il programma di studi; ● garantire che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente per la sicurezza online; ● garantire che sia tenuto un registro di incidenti di sicurezza online; ● facilitare la formazione e la consulenza per tutto il personale; ● coordinare con le autorità locali e le agenzie competenti; ● controllare la condivisione di dati personali; ● controllare l'accesso a materiali illegali/inadeguati; ● controllare probabili azioni di cyberbullismo.
L'Animatore Digitale ed il suo team	● pubblicare la E-Safety Policy sul sito della scuola; ● diffusione della E- Safety Policy; ● garantire che tutti i dati relativi agli alunni pubblicati sul sito siano sufficientemente tutelati.
Gli insegnanti	● inserire tematiche legate alla sicurezza on-line in tutti gli aspetti del programma di studi e di altre attività scolastiche; ● supervisionare e guidare gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono la tecnologia on-line; ● garantire che gli alunni siano pienamente consapevoli delle capacità di ricerca e siano pienamente consapevoli dei problemi legali relativi ai contenuti elettronici come ad esempio le leggi sul copyright.
Il personale scolastico	● comprendere e contribuire a promuovere politiche di e-sicurezza ; ● essere consapevoli dei problemi di sicurezza on-line connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili; monitorare l'uso di dispositivi tecnologici e attuare politiche scolastiche per quanto riguarda questi dispositivi; ● segnalare qualsiasi abuso sospetto o problema ai responsabili della sicurezza online; ● usare comportamenti sicuri, responsabili e professionali nell'uso della tecnologia; garantire che le comunicazioni digitali con gli studenti dovrebbero essere a livello professionale e solo attraverso i sistemi scolastici, non attraverso meccanismi personali, per esempio -mail, telefoni cellulari, ecc.

Gli alunni	● leggere, comprendere ed accettare la E- Safety Policy; ● avere una buona comprensione delle capacità di ricerca e la necessità di evitare il plagio e rispettare normative sul diritto d'autore; ● capire l'importanza di segnalare abusi, o l'uso improprio o l'accesso a materiali inappropriati; ● sapere quali azioni intraprendere se loro o qualcuno che conoscono si sente preoccupato o vulnerabile quando si utilizza la tecnologia on-line; ● conoscere e capire la politica relativa all'uso dei telefoni cellulari, fotocamere digitali e dispositivi portatili; ● conoscere e capire la politica della scuola sull'uso di immagini e il cyberbullismo; capire l'importanza di adottare buone pratiche di sicurezza on-line quando si usano le tecnologie digitali fuori dalla scuola; ● assumersi la responsabilità di conoscere i benefici e i rischi di utilizzo di Internet e di altre tecnologie in modo sicuro, sia a scuola che a casa.
I genitori	● sostenere la scuola nel promuovere la sicurezza online e approvare l'accordo di E-Safety Policy con la scuola; ● leggere, comprendere e controfirmare il suddetto accordo; ● accedere al sito web della scuola in conformità con quanto stabilito dalla stessa.

Al fine di garantire una gestione il più possibile corretta, la scuola attua le seguenti strategie:

Il Dirigente Scolastico, sentiti i responsabili, si attrezza per evitare comportamenti come:

- scaricare file video-musicali protetti da copyright;
- visitare siti non necessari ad una normale attività didattica (per esempio siti di shopping online);
- alterare i parametri di protezione dei computer in uso;
- utilizzare la rete per interessi privati e personali che esulano dalla didattica;
- non rispettare le leggi sui diritti d'autore;
- navigare su siti non accettati dalla protezione interna alla scuola.

Disposizioni, comportamenti, procedure:

- Il sistema informatico è periodicamente controllato dai responsabili (DSGA e docente responsabile su nomina del Dirigente Scolastico).
- La scuola può controllare periodicamente i file utilizzati, i file temporanei e i siti visitati da ogni macchina.
- E' vietato installare e scaricare da Internet software non autorizzati.
- É vietato scaricare file che potrebbero essere protetti da diritti d'autore (utilizzare software come "emule" per effettuare il download di filmati protetti dal diritto d'autore è un'attività illegale, ma è anche un'attività che da un punto di vista tecnico va ad intasare la rete impedendo ad altri utenti di lavorare).
- Al termine di ogni collegamento la connessione deve essere chiusa.
- Verifiche antivirus sono condotte periodicamente sui computer e sulle unità di memorizzazione di rete.
- L'utilizzo di CD, chiavi USB deve essere autorizzato dal docente e solo previa scansione antivirus per evitare qualsiasi tipo di infezione alla rete d'Istituto.
- La scuola si riserva di limitare il numero di siti visitabili e le operazioni di download.
- Il materiale didattico dei docenti può essere messo in rete, anche su siti personali collegati all'Istituto, sempre nell'ambito del presente regolamento e nel rispetto delle leggi.

Condivisione e comunicazione della Policy all'intera comunità scolastica.

La E-Safety Policy d'Istituto si applica a tutti i componenti della scuola, compreso il personale, gli studenti, i genitori, gli utenti della comunità, che ne hanno accesso.

La Policy sarà comunicata al personale, agli alunni, alla comunità nei seguenti modi:

- pubblicazione della E-Safety Policy sul sito della scuola.

Gestione delle infrazioni alla Policy:

La scuola prenderà tutte le precauzioni necessarie per garantire la sicurezza on-line.

Al personale e agli alunni saranno date informazioni sulle infrazioni in uso e le eventuali sanzioni.

2. Formazione e Curricolo

Il Piano Nazionale Scuola Digitale (PNSD) ha l'obiettivo di modificare gli ambienti di apprendimento per rendere l'offerta formativa di ogni istituto coerente con i cambiamenti della società della conoscenza e con le esigenze e gli stili cognitivi delle nuove generazioni. Il PNSD, con valenza pluriennale, è quindi un'opportunità per innovare la Scuola, adeguando non solo le strutture e le dotazioni tecnologiche a disposizione dei docenti e dell'organizzazione, ma soprattutto le metodologie didattiche e le strategie usate con gli alunni in classe.

Il D.M. 851 del 27 ottobre 2015, in attuazione dell'art.1, comma 56 della legge 107/2015, ne ha previsto l'attuazione al fine di:

- migliorare le competenze digitali degli studenti anche attraverso un uso consapevole delle stesse;
- implementare le dotazioni tecnologiche della scuola al fine di migliorare gli strumenti didattici e laboratoriali ivi presenti;
- favorire la formazione dei docenti sull'uso delle nuove tecnologie ai fini dell'innovazione didattica;
- individuare un Animatore Digitale ed un *team* per l'innovazione digitale che supporti ed accompagni adeguatamente l'innovazione didattica, nonché l'attività dell'animatore Digitale;
- partecipare a bandi nazionali ed europei per finanziare le suddette iniziative;

Curricolo sulle competenze digitali per gli studenti

Nell'ambito del PNSD questa scuola si propone un programma di progressiva educazione alla sicurezza, online come parte del curriculum scolastico. Si impegna a sviluppare una serie di competenze e comportamenti adeguati alle età degli alunni e ad esperienza, tra cui:

- programmare attività e far partecipare gli alunni a laboratori di Coding;
- sviluppare una serie di strategie per valutare e verificare le informazioni prima di accettare l'esattezza;
- essere a conoscenza che l'autore di un sito web/pagina può avere un particolare pregiudizio;
- sapere come restringere o affinare una ricerca;
- capire il comportamento accettabile quando si utilizza un ambiente online, vale a dire, essere educato, non utilizzare comportamenti inappropriati, mantenere le informazioni personali private;
- capire come le fotografie possono essere manipolate e individuare contenuti web in grado di attrarre il tipo sbagliato di attenzione;
- capire perché “amici” online potrebbero non essere chi dicono di essere e di comprendere perché dovrebbero fare attenzione in un ambiente online;
- capire il motivo per cui non dovrebbero inviare o condividere resoconti dettagliati delle loro vite personali e informazioni di contatto;
- capire il motivo per cui non devono pubblicare foto o video di altri senza il loro permesso;
- sapere di non scaricare alcun file - come i file musicali - senza permesso;
- comprendere l'impatto di bullismo online, sexting, grooming e sapere come cercare aiuto se sono in pericolo;
- sapere come segnalare eventuali abusi tra cui il bullismo on-line e come a chiedere aiuto ai docenti, ai genitori, se si verificano problemi quando si utilizzano le tecnologie Internet;
- utilizzare con attenzione Internet per garantire che si adatti alla loro età e supporti gli obiettivi di apprendimento per le aree curriculari specifiche.

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

Nell'ambito del PNSD questa scuola ha previsto:

- individuazione e formazione di un Animatore Digitale che come docente accompagnerà il Dirigente Scolastico e il Direttore S.G.A. nell'attuazione degli obiettivi e delle innovazioni previste dal PSND;
- formazione dei docenti all'utilizzo del registro elettronico e dello scrutinio elettronico;
- realizzazione/ampliamento della rete WI-FI/LAN dei 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;
- monitoraggio del piano digitale di Istituto e dei risultati conseguiti;
- si assicura che il personale sa come inviare o ricevere dati sensibili o personali e comprendere l'obbligo di crittografare i

dati dove la sensibilità richiede protezione degli stessi;

- offre una formazione a disposizione del personale in materia di sicurezza on-line attraverso corsi di formazione e/o aggiornamento;
- fornisce, come parte del processo di induzione, tutto il nuovo personale con informazioni e indicazioni sulla E-Safety Policy d'Istituto.

Sensibilizzazione delle famiglie.

Questa scuola esegue un programma continuativo di orientamento e di informazione per i genitori, tra cui:

- presentare ai genitori, i cui figli si scrivono nel nostro Istituto, il Regolamento della Policy, al fine di garantire che i principi di comportamento sicuro on-line siano chiari;
- distribuire volantini di informazione e pubblicazioni sul sito della scuola;
- fornire informazioni sui siti nazionali di sostegno per i genitori, quali il sito www.generazioniconnesse.it.

3. Gestione dell'infrastruttura e della strumentazione ICT della scuola.

Sito web della scuola

L'Istituto dispone di un proprio spazio web e di un proprio dominio: www.iccastelverderoma.edu.it

L'Istituto gestisce un proprio sito web nello spazio di proprietà. La gestione del sito della scuola e la rispondenza alle normative per quanto concerne i contenuti (accuratezza, appropriatezza, aggiornamento) e le tecniche di realizzazione e progettazione è a cura del Webmaster. La scuola detiene i diritti d'autore dei documenti che si trovano sul proprio sito o di quei documenti per i quali è stato chiesto ed ottenuto il permesso dall'autore proprietario. Le informazioni pubblicate sul sito della scuola relative alle persone da contattare rispetteranno le norme vigenti sulla privacy.

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

Sicurezza Rete Lan

L'Istituto dispone di un dominio su rete locale (rete segreteria) cui accedono i computer dell'amministrazione, tali postazioni sono su una rete locale isolata dal resto della rete d'Istituto (rete didattica). Il collegamento di computer portatili 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 regolarmente aggiornati.

La memorizzazione dei documenti e delle impostazioni personali è garantita attraverso il meccanismo di profilo mobili di Windows, che archivia centralmente sul server di dominio i dati, e li rende disponibili in tutte le postazioni legate alla didattica (laboratori, sale insegnanti, postazioni per studenti e docenti). Su questi dispositivi non è garantito alcun servizio di backup, pertanto si consiglia di fare copia su un supporto personale (Pendrive, Hard Disk esterni, o altro) dei propri dati.

Per quanto concerne la rete amministrativa, lo storage è garantito da backup automatico su altra postazione.

Sicurezza della rete senza fili (Wireless — WiFi)

Nell'Istituto è presente una rete con tecnologia senza fili. L'ottenimento delle credenziali è riservato al personale dell'Istituto e ospiti. Le regole di comportamento sono analoghe a quelle per la connessione alle reti cablate di Istituto.

4. Strumentazione personale

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

Come da Regolamento d'Istituto agli studenti è vietato l'utilizzo del cellulare all'interno della scuola. Per quanto concerne l'utilizzo dei tablet, questi possono essere utilizzati solo alla presenza del docente e per ragioni prettamente scolastiche.

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.

5. Prevenzione, rilevazione e gestione dei casi.

Prevenzione

Principi generali:

1. Internet favorisce la libertà d'espressione e, quando si entra a far parte di una community o di un servizio dove interagiscono più utenti, vanno considerati abusi meritevoli di segnalazione solo i contenuti palesemente impropri o illeciti e non tutti quei contenuti con cui semplicemente non si è d'accordo o non piacciono.
2. Quando si inizia a navigare tra i servizi dei Social Network e le applicazioni web tipo YouTube, Facebook etc., bisogna informarsi subito su quali sono i diritti e i doveri dell'utente, leggendo il regolamento, tenendosi aggiornati, esplorando i siti informativi e istituzionali che affrontano queste tematiche.
3. Se si condividono informazioni personali, bisogna farlo scegliendo con cura che cosa rendere pubblico e cosa rendere privato. E' indispensabile scegliere con attenzione le amicizie con cui accrescere la propria rete e i gruppi a cui aderire, proteggendo la propria identità digitale con password complesse e usando una domanda di recupero password dalla risposta non banale.
4. Se si condividono elementi multimediali o informazioni che riguardano più persone è necessario avere il permesso di ciascun utente coinvolto prima di effettuare la pubblicazione. Non bisogna pubblicare su YouTube video girati di nascosto e dove sono presenti persone filmate senza il loro consenso.
5. Bisogna contribuire a rendere il Web un luogo sicuro, pertanto ogni volta che un utente commette involontariamente un abuso o un errore, pubblicando del materiale illecito, non idoneo o offensivo, bisogna contattarlo e fornire le spiegazioni relative alle regole, diffondendo così i principi della sicurezza.
6. Ogni abuso subito o rilevato nella navigazione, deve essere segnalato tramite i canali e gli strumenti offerti dal servizio, indicando in modo semplice i riferimenti per ottenere tempestivamente la rimozione del contenuto (abuso, data, ora, utenti e servizio coinvolti). Tutti i social network garantiscono la possibilità di segnalare materiale inopportuno mediante semplici operazioni da compiere direttamente sul sito. Prima di trasformare un incidente o una "bravata" in una denuncia alle autorità competenti avvalersi della modalità di segnalazione che non obbliga le parti in causa a conseguenze penali e giudiziarie che possono durare anni.

Scuola e Famiglia possono essere determinanti nella diffusione di un atteggiamento mentale e culturale che consideri la diversità come una ricchezza e che educhi all'accettazione, alla consapevolezza dell'altro, al senso della comunità e della responsabilità collettiva. Occorre, pertanto, rafforzare e valorizzare la collaborazione tra scuola e famiglia: la scuola è chiamata ad adottare misure atte a prevenire e contrastare ogni forma di violenza e di prevaricazione; la famiglia è chiamata a collaborare, non solo educando i propri figli ma anche vigilando sui loro comportamenti.

Per definire una strategia ottimale di prevenzione e di contrasto, le esperienze acquisite e le conoscenze prodotte vanno contestualizzate alla luce dei cambiamenti, che hanno profondamente modificato la società, sul piano etico, sociale e culturale e ciò comporta una valutazione ponderata delle procedure adottate per riadattarle in ragione di nuove variabili, assicurandone in tal modo l'efficacia.

La forma online del bullismo ha però alcune caratteristiche peculiari che lo rendono pericoloso perché:

il cyberbullismo è pervasivo: il cyberbullo può raggiungere la sua vittima in qualsiasi momento e in qualsiasi luogo. La possibilità di avere smartphone sempre accesi e spesso connessi ad internet permette al cyberbullo di aggredire la sua vittima ogni volta che lo desidera;

è un fenomeno persistente: il materiale diffamatorio pubblicato su internet può rimanere disponibile online anche per molto tempo;

spettatori e cyberbulli sono potenzialmente infiniti: le persone che possono assistere ad episodi di cyberbullismo sono potenzialmente illimitate e molti possono essere cyberbulli, anche solo condividendo o promuovendo l'episodio di cyberbullismo, che finisce per replicarsi (ad esempio sulle bacheche dei profili che i ragazzi hanno sui social network) in modo incontrollabile.

Azioni

La scuola si impegna a:

- riconoscere il Dirigente Scolastico come titolare del trattamento di dati personali secondo la Legge sulla privacy (art. 41 f del D.Lgs. 196/2003);
- riconoscere come responsabili della sicurezza online il DSGA ed un docente su nomina del Dirigente Scolastico;

I docenti si impegnano a:

- accompagnare gli alunni nella navigazione in Rete, coinvolgendoli nell'esplorazione delle opportunità e dei rischi, con attività calendarizzate dall'inizio dell'anno;
- approfondire, con attività mirate in classe, la conoscenza del fenomeno del bullismo e del cyber bullismo;
- mantenere viva una task-force interna all'istituto, che possa progettare attività formative sul fenomeno del cyberbullismo e calendarizzarle per tutta la comunità scolastica;
- confrontarsi con gli altri insegnanti della classe, della scuola o con esperti del territorio;
- rivolgersi alla helpline di generazioni connesse (www.generazioniconnesse.it).

I genitori si impegnano a:

- prendere visione della E-Safety Policy messa a disposizione di docenti, genitori ed alunni sul sito della scuola;
- seguire le azioni promosse dalla scuola per un uso corretto della rete;

Gli alunni si impegnano a:

- prendere visione della E-Safety Policy pubblicata sul sito web della scuola;
- rispettare le regole per un uso corretto della tecnologia;
- denunciare qualsiasi caso di abuso online.

Rilevazione e gestione dei casi

Nel caso in cui un docente o qualsiasi operatore della scuola venga a conoscenza di fatti che possano essere riconducibili ad una condotta di cyber bullismo deve tempestivamente informare il Dirigente scolastico o un suo sostituto e/o il referente d'istituto.

L'obiettivo a lungo termine, che come comunità scolastica ci poniamo, è quello di creare una memoria condivisa non solo di ciò che accade nella scuola rispetto al web, ma anche di strutturare una fonte esemplificativa che possa orientare sempre più e sempre meglio le azioni di contrasto ad episodi che, nel tempo, potrebbero ripetersi.

Per poter tenere traccia di ciò che è avvenuto rispetto ai comportamenti degli alunni online e di come è stato gestito il problema, la scuola si riserva di utilizzare il "Diario di Bordo" messo a disposizione sul sito www.generazioniconnesse.it (Allegato n.1).

La Scuola si impegna inoltre ad organizzare le seguenti attività di prevenzione al fenomeno:

- ❖ organizzazione di Corsi di formazione per docenti;
- ❖ partecipazione da parte di docenti a convegni e seminari sul tema del bullismo e del cyberbullismo;
- ❖ interventi di consulenza e supporto - su richiesta da parte della scuola - relativamente a casi di cyberbullismo.

Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi

Scuola_____ Anno Scolastico_____

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

ALLEGATO 1

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

Ogni volta che un componente del personale o studente viola la E-Safety Policy, la decisione finale sul livello di sanzioni è di competenza del Dirigente Scolastico, se la violazione è a carico di uno studente la competenza è del Consiglio di classe presieduto dal Dirigente scolastico e rifletterà le procedure comportamentali e disciplinari della scuola.
Di seguito sono fornite solo come esemplificazione:

STUDENTI:

INFRAZIONI	**INTERVENTO E POSSIBILI SANZIONI**
● L'uso di siti non-educativi durante le lezioni. ● L'utilizzo non autorizzato di e-mail. ● L'uso non autorizzato del telefono cellulare (o altre nuove tecnologie) durante l'intera permanenza a scuola. ● Uso di instant messaging/siti di social networking.	Fare riferimento all'insegnante della classe/docente responsabile della sicurezza online/docente referente per il cyberbullismo/Dirigente Scolastico Possibili sanzioni: 1. allontanamento dall'attività laboratoriale; 2. invito a riporre il telefono fino a fine orario scolastico; 3. sospensione dalle lezioni 4. rimozione dei diritti di accesso a Internet per un periodo; 5. contattare le autorità competenti tramite il referente dell'Istituto; 6. conservare le prove; 7. informare i provider di servizi di posta elettronica del mittente; 8. fare rapporto alle autorità competenti tramite il referente dell'Istituto dove si sospetti la pedofilia o altre attività illegali. La sanzione è graduale a seconda dell'infrazione. Si sottolinea che le infrazioni che costituiscono reato verranno denunciate alle Autorità competenti. La sospensione dalle lezioni fino a 15 giorni è di competenza del Consiglio di classe, oltre i 15 giorni è di competenza del consiglio di istituto.
● L'uso continuato di siti non-educativi durante le lezioni dopo essere stato avvertito. ● L'uso non autorizzato di e-mail dopo essere stato avvertito. ● L'uso non autorizzato del telefono cellulare (o altre nuove tecnologie), durante l'intera permanenza a scuola, dopo essere stato avvertito. ● L'uso continuato messaggistica/chat room istantanea, siti di social networking, newsgroup. ● L'uso di materiale offensivo.	
● Rovinare o distruggere deliberatamente i ● dati di qualcuno, violare la privacy altrui o ● messaggi inappropriati , video o immagini su un sito di social networking. ● Invio di un messaggio e-mail o MSN che è ● considerato molestia o azione di bullismo. ● Cercare di accedere a materiale offensivo o ● pornografico.	
● Invio di e-mail o messaggi di MSN considerati molestia o bullismo dopo essere stato avvertito. ● Accedere deliberatamente allo scaricamento o alla diffusione di qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofobico o violento. ● Trasmissione di materiale che viola i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati. ● Portare il nome della scuola in discredito.	

PERSONALE SCOLASTICO

INFRAZIONI	**POSSIBILI SANZIONI**
● L'uso di Internet per attività personali non legate allo sviluppo professionale (shopping online, e-mail personali, instant messaging ecc.). ● L'utilizzo di supporti di memorizzazione dei dati personali (ad esempio, chiavette USB) senza considerare l'accesso e l'adeguatezza di qualsiasi file memorizzato. ● Non implementare adeguate procedure di salvaguardia. ● Qualsiasi comportamento sul World Wide Web che compromette la professionalità del personale nella scuola e nella comunità. ● L'uso improprio di primo livello di sicurezza dei dati, ad esempio uso illecito di password. ● Violazione del copyright o della licenza per	Fare riferimento al docente responsabile della sicurezza online /DSGA /Dirigente Scolastico Azioni di salvaguardia: 1. rimuovere il PC e posizionarlo in un luogo sicuro per garantire che non vi sia alcun ulteriore accesso; 2. far verificare tutte le attrezzature per garantire che non vi sia alcun rischio di alunni che accedono a materiali inappropriati nella scuola; 3. contattare e fare rapporto alle autorità competenti. La sanzione è commutata a seguito dell'iter procedurale stabilito per i dipendenti della Pubblica Amministrazione.

l'installazione di software .	
● Gravi danni intenzionali all'hardware o software del computer. ● Qualsiasi tentativo deliberato di violare la protezione dei dati o di sicurezza informatica. ● Creare, accedere, scaricare e diffondere deliberatamente qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofobico o violento. ● Ricevere o trasmettere materiale che viola i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati. Portare il nome della scuola in discredito	

Come saranno informati il personale e gli studenti di queste procedure?

- La E-Safety Policy sarà resa disponibile sul sito dell'Istituto a studenti, personale scolastico e genitori
- Agli studenti sarà insegnato un uso responsabile della rete in modo tale che possano sviluppare "comportamenti sicuri".
- Informazioni su come segnalare azioni di bullismo o cyberbullismo saranno messe a disposizione dalla scuola per gli alunni, il personale e i genitori.