



MINISTERO DELL' ISTRUZIONE UNIVERSITÀ RICERCA
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
ISTITUTO COMPRENSIVO "MARTIN LUTHER KING"
VIA DEGLI ORAFI n° 30 - 00133 ROMA - DISTRETTO SCOLASTICO XVI
tel.06/2023327/2023663 - fax 06/2023327 C. M. RMIC83300C
e-mail RMIC83300C@ISTRUZIONE.IT - C.F. 9719797058
sito web www.icmlking.gov.it



Istituto Comprensivo Martin Luther King

E - SAFETY POLICY

1. Introduzione

Scopo della Policy

L'utilizzo sempre più diffuso delle TIC (Tecnologie dell'Informazione e della Comunicazione) all'interno degli ambienti scolastici da parte di tutti i componenti della comunità educativa pone l'accento sulla necessità di educare ad un loro uso corretto e responsabile.

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.

L'E-Safety dell'Istituto Martin Luther King, insieme agli altri regolamenti d'Istituto e alle politiche relative ai comportamenti degli alunni definisce pertanto:

- misure di prevenzione e di gestione di situazioni problematiche relative all'uso delle tecnologie digitali;
- misure atte a facilitare e promuovere l'utilizzo positivo delle TIC nella didattica e negli ambienti scolastici.

Ruoli e Responsabilità.

L'Istituto Comprensivo Martin Luther King ha costituito un gruppo di lavoro, formato dall'Animatore digitale, dal Team digitale e dal Referente per il Bullismo e il Cyberbullismo, che si occupa della stesura e del monitoraggio della E – Policy approvata dal Dirigente Scolastico e dal Collegio dei Docenti.

Il seguente documento definisce in modo chiaro i ruoli e le responsabilità di ogni membro della comunità educante.

Dirigente Scolastico

Il ruolo del Dirigente scolastico nel promuovere l'uso consentito delle tecnologie e di internet include i seguenti compiti:

- Garantire il rispetto della E-policy d'Istituto.
- Garantire la sicurezza (tra cui la sicurezza on-line) dei membri della comunità scolastica.
- Garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line.
- Essere a conoscenza delle procedure per la prevenzione, rilevazione e gestione di strategie utili per individuare casi di rischio nell'utilizzo delle TIC a scuola.
- Garantire che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della comunicazione (TIC).

- Comprendere e seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.
- Ricevere relazioni periodiche di monitoraggio dal Referente del bullismo e del cyber bullismo, dall'Animatore digitale e /o dal Team digitale

Animatore digitale

Il ruolo dell'Animatore digitale nel promuovere l'uso consentito delle tecnologie e di internet implica i seguenti compiti:

- Coordinare e mantenere contatti con il Team digitale, con il Referente del bullismo e del cyberbullismo, con le autorità e gli enti esperti.
 - Relazionare periodicamente il lavoro del gruppo con il Dirigente Scolastico.
 - 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 gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti.
 - Coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".
- Si relaziona con la Ditta che gestisce l'assistenza tecnico-informatica per definire le misure di sicurezza informatica più opportune; riferisce al Dirigente scolastico situazioni o problemi di particolare rilevanza su cui intervenire.

Team digitale

Il ruolo del Team digitale nel promuovere l'uso consentito delle tecnologie e di internet implica i seguenti compiti:

- Definire e revisionare le politiche e i documenti di E-Safety.
- Promuovere la consapevolezza e l'impegno, per la salvaguardia relativa alle tecnologie, di tutta la comunità educante.
- Diffondere la conoscenza delle procedure per la prevenzione, rilevazione e gestione di strategie utili per individuare casi di rischio nell'utilizzo delle TIC a scuola.
- Assicurare che nel curriculum scolastico vengano inseriti i diversi aspetti della sicurezza in internet.
- Monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola (condivisione di dati personali, accesso a materiali illegali e/o inadeguati, cyber – bullismo, ecc. ...).

Referente bullismo e cyberbullismo

Il ruolo del Referente del bullismo e cyberbullismo (Legge n. 71 del 29/05/2017, Disposizioni a tutela dei minori per la prevenzione del fenomeno del cyberbullismo) nel promuovere l'uso consentito delle tecnologie e di internet implica i seguenti compiti:

Coordinare la Commissione preposta.

- Ascoltare e aiutare gli alunni per ridurre e prevenire fenomeni di illegalità e inciviltà o chi si trova in difficoltà perché oggetto di prevaricazioni online.
- Intervenire nei confronti di chi fa un uso inadeguato della rete e dei cellulari, ascoltando eventuali problemi e fornendo consigli.
- Sensibilizzare, dare informazioni agli alunni e alle famiglie su quelli che sono i rischi della rete, comunicandogli le azioni che la scuola mette in atto in caso di fenomeni di bullismo e cyberbullismo.
- Informare gli insegnanti della eventuale presenza di casi di bullismo e cyberbullismo.
- Convocare, sentito il parere del Dirigente Scolastico, gli interessati di atti di bullismo e cyberbullismo per adottare misure di assistenza alla vittima e sanzioni, in base alla gravità del fatto, e percorsi rieducativi per l'autore.
- Promuovere e pubblicizzare le iniziative di formazione rivolte agli alunni, ai genitori, ai docenti e al personale ATA dell'Istituto comprensivo.
- Coordinare le iniziative di prevenzione e di contrasto del bullismo e del cyberbullismo, anche in collaborazione con Forze di Polizia, associazioni e centri di aggregazione giovanili presenti nel territorio.
- Coordinare e curare il monitoraggio delle azioni intraprese per combattere i fenomeni di bullismo e cyberbullismo.
- Mettere a disposizione la normativa vigente e i materiali di approfondimento.

Direttore dei servizi generali e amministrativi

Il ruolo del direttore dei servizi generali e amministrativi include i seguenti compiti:

- Assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnologica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;
- Garantire il funzionamento dei diversi canali di comunicazione dell'Istituto all'interno della comunità scolastica e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni nell'ambito dell'utilizzo delle TIC.

Lo staff

Il ruolo dello Staff implica i seguenti compiti:

- Promuovere le politiche di E–Safety dell’Istituto.
- Essere consapevole dei problemi di sicurezza correlati all’utilizzo delle nuove tecnologie digitali, monitorandone l’utilizzo e applicando le vigenti politiche scolastiche in materia.
- Segnalare al Referente del bullismo e del cyberbullismo ogni tipo di abuso o di problema.
- Favorire comportamenti responsabili e sicuri nell’utilizzo della tecnologia.

Docenti

Il ruolo del personale docente e di ogni figura educativa che lo affianca implica i seguenti compiti:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell’utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l’utilizzo scorretto e pericoloso delle TIC e di internet;
- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore (privacy, copyright...);
- 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;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo all’Animatore digitale 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;
- segnalare al Dirigente scolastico, qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all’utilizzo delle tecnologie digitali o di internet, per l’adozione delle procedure previste dalle norme

Tecnico esterno

Il ruolo del tecnico esterno implica i seguenti compiti:

- Eseguire una manutenzione periodica dell’infrastruttura tecnologica dell’Istituto.
- Fare un controllo periodico al sistema di sicurezza dei dati (firewall, filtri, server per il controllo degli account...).

Studenti

Il ruolo degli studenti implica i seguenti compiti:

- Leggere, comprendere e aderire all'E-Safety dell'Istituto in relazione al proprio grado di maturità e di apprendimento, per un utilizzo responsabile e corretto delle TIC.
- avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;
- comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;
- adottare condotte rispettose degli altri anche quando si comunica in rete
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti, al Referente del bullismo e cyber-bullismo, al Dirigente scolastico e ai genitori.

Genitori

Il ruolo dei genitori implica i seguenti compiti:

- Leggere, comprendere, firmare e aderire all'E-Safety dell'Istituto per un utilizzo responsabile e corretto delle TIC da parte dei propri figli.
- Sostenere la linea di condotta dell'Istituto nei confronti dell'utilizzo delle tecnologie dell'informazione e delle comunicazioni nella didattica.
- Concordare con i docenti e con il Referente del bullismo e del cyberbullismo linee di intervento coerenti e di carattere educativo in relazione all'utilizzo delle TIC soprattutto in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitale o della rete.
- Seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dalla scuola, in particolare controllare l'utilizzo del pc e di internet;
- Fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e del telefonino in generale
- Partecipare alle iniziative di formazione proposte dall'istituto in materia di sicurezza di rete.

Condivisione e comunicazione della Policy all'intera comunità scolastica

Vista l'importanza di un corretto uso delle TIC e della rete internet e per diffondere la consapevolezza delle norme di comportamento e delle conseguenti sanzioni in caso di cattivo utilizzo, l'E-Safety Policy verrà presentata e condivisa con l'intera comunità scolastica avvalendosi di diversi mezzi e con l'aiuto di tutte le componenti dell'Istituto

Condividere e comunicare la politica di E- Safety agli alunni

- Presentazione della E-Safety alle classi quarte e quinte della scuola Primaria e a tutte le classi della scuola Secondaria di Primo grado.

- Affissione dell'elenco delle regole per la sicurezza on-line in tutte le aule e laboratori con accesso ad internet.
- Riflessione sugli aspetti della sicurezza in rete per i quali gli alunni risultano più esposti (cyber-bullismo, grooming, sexting,,).).
- Formazione sull'argomento in classe nelle ore curricolari/extracurricolari, con i docenti e/o con esperti esterni.

Condividere e comunicare la politica di E-Safety ai genitori

- Pubblicazione della versione integrale della E-Safety sul sito web dell'Istituto.
- Collaborazione tra scuola e famiglia sulla condivisione di regole comuni sulla sicurezza nell'uso delle TIC e di internet.
- Formazione sull'argomento in occasione degli incontri scuola-famiglia, collegiali, individuali e con esperti esterni.
- Supporto alle famiglie da parte dell'Animatore digitale e del Referente del bullismo e cyber-bullismo per l'individuazione di strumenti adeguati a garantire la navigazione sicura anche a casa.

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;
- Per proteggere tutto il personale e gli alunni, la scuola metterà in atto una linea di condotta di utilizzo accettabile, controllato e limitato alle esigenze didattiche essenziali;
- Il personale docente sarà reso consapevole del fatto che il traffico in internet può essere monitorato e si potrà risalire al singolo utente registrato;
- Un'adeguata informazione/formazione on-line del personale docente nell'uso sicuro e responsabile di internet, sia professionalmente che personalmente, sarà fornita a tutto il personale, anche attraverso il sito web della scuola;
- Il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC sarà supervisionato dall'Animatore digitale, che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici;
- L'Animatore digitale metterà in evidenza on-line utili strumenti che il personale potrà usare con gli alunni in classe. Questi strumenti varieranno a seconda dell'età e della capacità degli alunni;
- 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.

Gestione delle infrazioni alla Policy.

Alunni

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali di internet di cui si dispone per la didattica, in relazione alla fascia di età considerate, sono prevedibilmente le seguenti:

- 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 condivisione di immagini intime o troppo spinte;
- la comunicazione incauta e senza permesso con sconosciuti;
- il collegamento a siti web non indicati dai docenti.
- Mancato rispetto della Netiquette (regole di scrittura in rete)

Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo dell'alunno.

Infatti più gli alunni sono piccoli, più i comportamenti "da correggere" sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, che devono essere compresi e orientati proprio dagli educatori, nella prospettiva del raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno.

Sono previsti pertanto da parte dei docenti provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento, quali:

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

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, 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.

La valutazione spetta al Dirigente Scolastico e all'equipe pedagogica/Consiglio di classe. Violazioni gravi e/o ripetute delle norme, oltre a provvedimenti di natura didattica potranno comportare il divieto temporaneo o anche, nei casi più gravi, permanente di accesso alle risorse informatiche e alla rete. Rimangono, inoltre, applicabili ulteriori sanzioni disciplinari e azioni civili per danni, nonché l'eventuale denuncia all'autorità giudiziaria qualora la violazione si configuri come reato.

Personale scolastico

Tutto il personale scolastico e in particolare i docenti possono incorrere in potenziali infrazioni se utilizzano in modo improprio e scorretto le tecnologie digitali o internet.

Per evitare ciò devono :

- utilizzare le tecnologie e i servizi della scuola solo e unicamente per attività connesse all'insegnamento o ad attività inerenti al profilo professionale.
- Comunicare elettronicamente con i genitori e gli alunni in modo compatibile con il ruolo professionale.
- Porre particolare attenzione al rispetto del trattamento dei dati personali degli alunni come previsto dalle norme relative alla privacy.
- Essere ligi nella conservazione delle password assegnate, al fine di evitare il loro utilizzo improprio da parte di terze persone.
- Curare la formazione degli alunni sull'utilizzo corretto e responsabile delle TIC.
- Vigilare durante l'utilizzo delle TIC da parte degli alunni e segnalare situazioni critiche al Dirigente scolastico e ai preposti.

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 successivi accertamenti.

I provvedimenti disciplinari e le sanzioni sono quelle previste dalla legge e dai contratti di lavoro.

Genitori

La collaborazione tra scuola e famiglia è fondamentale per aiutare gli alunni a utilizzare in modo corretto e responsabile le TIC e internet.

In particolare i genitori a casa dovrebbero evitare alcuni comportamenti che possono favorire un uso scorretto delle tecnologie come :

- 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, del cellulare, dello smartphone o del tablet in comune con gli adulti che possono conservare in memoria materiali non idonei;

In caso di infrazioni, i genitori possono essere convocati a scuola per concordare misure educative oppure essere sanzionati a norma di legge in base alla gravità dei comportamenti tenuti dai propri figli.

La scuola si rende disponibile a collaborare con la famiglia qualora vengano comunicate problematiche sorte al di fuori del contesto scolastico per aiutare gli alunni nel loro cammino di crescita.

Monitoraggio dell'implementazione della Policy e suo aggiornamento.

Il monitoraggio dell'implementazione della policy e del suo eventuale aggiornamento sarà svolto ogni anno. Tale monitoraggio sarà curato dal Dirigente scolastico con la collaborazione dell'Animatore digitale e dai docenti delle classi, tramite questionari e conversazioni. Sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di internet. Il monitoraggio sarà rivolto anche agli insegnanti, al fine di valutare l'impatto della policy e la necessità di eventuali miglioramenti.

Integrazione della Policy con Regolamenti esistenti

La presente E-Safety si integra pienamente con obiettivi e contenuti dei seguenti documenti, che specificano il contesto di attuazione delle politiche dell'Istituto comprensivo per un uso efficace e consapevole del digitale nella didattica:

- PTOF, incluso il piano per l'attuazione del PNSD;
- Regolamento interno d'Istituto;
- Regolamento di accesso e di uso ai laboratori multimediali. (allegato)
- Regolamento di utilizzo della LIM e dei computer in classe. (allegato

In applicazione:

- ✓ “Linee di orientamento Contro il bullismo e il cyberbullismo” (MIUR – 13 Aprile 2015).
- ✓ “Piano Nazionale per la prevenzione del bullismo e del cyberbullismo a scuola (MIUR 2016/2017).
- ✓ “Legge n. 71 del 29/05/2017, Disposizioni a tutela dei minori per la prevenzione del fenomeno del cyberbullismo”.

2. Formazione e Curricolo

Curricolo sulle competenze digitali degli alunni

Inserita nelle otto Competenze chiave di cittadinanza attiva, indicate dal Consiglio di Lisbona del 2000, “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 del 2012. Si ritrovano abilità e conoscenze che fanno capo alla competenza digitale in tutte le discipline e tutte concorrono a costruirla.

La competenza digitale fa riferimento alla capacità di comprendere e sfruttare l’effettivo potenziale delle tecnologie in ottica di costruzione, di conoscenza e di promozione della partecipazione e dell’inclusione; il rapporto con le tecnologie digitali guarda così a forme di uso consapevole, critico e creativo.

Il Piano 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.

Nell’ambito del PNSD, questo Istituto si propone un programma di progressiva educazione alla sicurezza online, come parte del curriculum scolastico e si impegna a sviluppare una serie di competenze e comportamenti adeguati all’età degli alunni e alla loro esperienza. La scuola ha già proposto e continuerà ad offrire laboratori di coding e di tinkering.

Ha iniziato a sviluppare una serie di strategie per aiutare gli alunni ad adoperare un comportamento corretto quando si utilizza un ambiente online e a non inviare o condividere materiali inadeguati.

Ha organizzato incontri per far comprendere l’impatto del bullismo online, sexting, grooming e sapere come cercare aiuto se si presentano situazioni di pericolo. Si sta, inoltre, adoperando per garantire che Internet si adatti all’età degli alunni e supporti gli obiettivi di apprendimento per le aree curriculari specifiche

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 dall’istituzione o dalle scuole associate in rete di distretto e di ambito; possiede generalmente una buona base di competenze e nel caso delle figure di sistema, anche di carattere specialistico. E’ inoltre disponibile ad aggiornarsi per mantenere al passo la propria formazione, in rapporto al rinnovo della dotazione tecnologia e degli ambienti di apprendimento. Il percorso di formazione in itinere prevede:

- momenti di autoaggiornamento.
- Momenti di formazione personale e /o collettiva organizzate dall’Animatore digitale e dal Team digitale.
- Formazione dei docenti all’utilizzo del registro elettronico e dello scrutinio elettronico.

- Somministrazione di un questionario rivolto ai docenti per la rilevazione dei “bisogni formativi” e per la “rilevazione delle competenze”.
- Partecipazione alle iniziative promosse dall’Amministrazione centrale e dalle scuole in rete di distretto e di ambito..
- Corsi on-line.

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

Anche il percorso della formazione specifica dei docenti sull’utilizzo consapevole e sicuro di Internet, può prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all’evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi.

Sarà predisposta una sezione online, sul sito d’Istituto: www.icmlking.gov.it, per la messa a disposizione e la condivisione di materiali finalizzati all’aggiornamento sull’utilizzo consapevole e sicuro di internet. Qui sarà 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, e link messi a disposizione dal sito “Generazioni connesse” con il contributo della Polizia di Stato, dei Carabinieri, del Telefono Azzurro e di altri enti o associazioni competenti in materia.

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 sezione 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.

Gestione dell’infrastruttura e della strumentazione ICT della

Accesso ad internet: filtri, antivirus e sulla navigazione.

L’accesso a internet è possibile e consentito esclusivamente per la didattica nei laboratori e nelle aule, per l’utilizzo del Registro Elettronico e per la comunicazione scolastica. E’ schermato da filtri (firewall) che impediscono il collegamento a siti appartenenti a black list consentendo il collegamento solo a siti idonei alla didattica. Sui pc client dei laboratori è impostato il controllo genitori, per limitare l’accesso ai giochi, per disciplinare l’orario di utilizzo delle postazioni.

Tutti gli operatori connessi ad internet devono rispettare le predette norme e la legislazione vigente applicata in materia. Gli utenti si impegnano a non consultare deliberatamente, conservare o diffondere documenti che possono ledere la dignità della persona (ai sensi degli artt. 173, 197, 261 CPS).

E’ proibito caricare e/o scaricare a/da internet files musicali, video e software che non siano attinenti alla propria mansione, come anche l’utilizzo della connessione ad internet per motivi strettamente personali.

E’, inoltre, vietato l’utilizzo dei pc della scuola per la memorizzazione di materiale privato e personale.

Gestione accessi (password, backup, ecc.)

L'accesso al sistema informatico per la didattica, server e internet, nel laboratorio multimediale è consentito al personale con un account dedicato, inserendo un nome utente e una password assegnati dall'Animatore Digitale o dal Referente. Il personale ha la responsabilità di mantenere i suddetti dati privati e se ne vieta la divulgazione. I docenti registrano il proprio accesso scrivendo sugli appositi registri la data, l'orario di utilizzo dei laboratori ed eventuali annotazione su riscontri di malfunzionamenti della strumentazione.

Non vi è un backup dei file elaborati, se non quello operato dai docenti interessati sui supporti rimovibili personali, che possono essere utilizzati solo dopo essere stati scansionati dall'antivirus. Le postazioni del laboratorio, così come quelle presenti nelle aule, funzionano come stazioni di lavoro e non come archivi.

E-mail

L'account di posta elettronica è solo quello istituzionale ed è utilizzato unicamente per comunicazioni, in entrata e in uscita, di carattere lavorativo. Gli utenti si impegnano a non diffondere informazioni che possono nuocere alla reputazione della scuola o essere contrarie alla morale o alle leggi in vigore.

Blog e sito web della scuola

Tutti i contenuti del sito dell'Istituto sono pubblicati dall'Animatore digitale che, insieme al Dirigente scolastico, ne valuta la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc.

Il Dirigente scolastico, inoltre, si assume la responsabilità che il sito web dell'Istituto sia conforme alle linee guida di legge, in particolar modo si assicura che il lavoro pubblicato sia frutto delle attività svolte dalla scuola e qualora fossero pubblicati lavori di altri renderà note le fonti utilizzate impegnandosi a richiedere l'autorizzazione degli stessi e a proibire la diffusione e/o la duplicazione di programmi e documenti coperti dal diritto d'autore.

Social network

Attualmente nella didattica non si utilizzano social network, né l'istituzione scolastica vi ha creato una pagina col proprio profilo o ha autorizzato il personale scolastico a utilizzarli per nome e per conto della stessa.

Protezione dei dati personali.

Il Dirigente e il personale scolastico da questi delegato sono responsabili 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 delle proprie funzioni. Il personale incaricato deve applicare la procedura sul trattamento dei dati personali su supporto cartaceo e su supporto informatico per la protezione e la sicurezza degli stessi.

I soggetti cui si riferiscono i dati personali hanno il diritto in base all'articolo 7 del D.lgs. n. 196/2003 di verificarne l'esattezza o l'aggiornamento o l'eventuale cancellazione.

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.

Ai sensi del Regolamento d'Istituto non è consentito agli alunni alcun uso di strumenti elettronici personali durante le lezioni. A tale disposizione fa eccezione il caso in cui l'uso sia espressamente autorizzato dal Dirigente scolastico, su richiesta del docente di classe, per lo svolgimento di attività educative/didattiche riguardanti la scuola o in casi di estrema e comprovata urgenza per comunicazioni tra gli alunni e le famiglie.

In questi casi, ogni studente è responsabile del proprio dispositivo e non può prendere in prestito dispositivi di altri. E', inoltre, vietato usare dispositivi di registrazione audio, videocamere o fotocamere (o dispositivi che li prevedano) per registrare o fare foto in classe senza il permesso del docente e senza il permesso della persona interessata.

Non è consentito l'utilizzo di internet per scopi diversi da quelli scolastici, scaricare musica, video e software da internet e giocare con i dispositivi.

L'Istituto si riserva il diritto di monitorare, controllare, ecc. ... le attività on-line degli alunni e di avvisare le Forze dell'Ordine quando lo ritenga necessario.

Per i docenti: gestione degli strumenti personali – cellulari, tablet ecc.

Durante le ore di lezione, ai docenti non è consentito l'utilizzo del cellulare o dello smartphone che non deve essere lasciato incustodito e non può essere prestato agli alunni.

E' consentito l'uso di altri dispositivi elettronici, ad integrazione di quelli forniti dalla scuola, e di internet per soli fini didattici.

E' vietato usare dispositivi di registrazione audio, videocamere o fotocamere (o dispositivi che li prevedano) per registrare o fare foto in classe senza il permesso del Dirigente scolastico e senza l'autorizzazione dei genitori.

Durante il restante orario di servizio è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente.

L'Istituto si riserva il diritto di monitorare le attività on-line degli utenti che utilizzano la rete wifi della scuola e controllare ogni comunicazione elettronica, avvisando le forze dell'ordine quando lo ritenga necessario.

L'uso improprio verrà sanzionato in base alla normativa vigente in materia.

Per il personale della scuola: gestione degli strumenti personali – cellulari, tablet ecc.

Durante l'orario di servizio al restante personale scolastico non è consentito l'uso di strumenti tecnologici personali salvo in caso di comunicazioni personali di carattere urgente.

L'uso improprio verrà sanzionato in base alla normativa vigente in materia.

Prevenzione, rilevazione e gestione dei casi

Rischi

<u>RISCHI</u>	Cyber-bullismo
	Grooming
	Sexting

I rischi effettivi in cui si può incorrere nell'utilizzo delle TIC a scuola da parte degli alunni derivano da un uso non corretto dei dispositivi elettronici personali e non, collegati ad internet. In particolare i rischi in rete più diffusi sono: **Cyberbullismo**, **Sexting** e **Grooming**.

Azioni di prevenzione

<u>Azioni</u>	Informare/formare sui rischi
	Controllo delle procedure
	Utilizzo di firewall, filtri, software specializzati e black list
	Collaborazione con gli enti esterni

I docenti svolgono attività di controllo degli alunni durante l'orario scolastico per evitare rischi a causa di un accesso non controllato o di un uso improprio di internet accompagnando gli alunni nella navigazione in Rete, coinvolgendoli nell'esplorazione delle opportunità e dei rischi.

Gli alunni e i genitori si impegnano a prendere visione della E-Safety Policy, a seguire le azioni promosse dalla scuola, a rispettare le regole per un uso corretto della Rete e a frequentare i corsi di formazione che la scuola organizzerà per la diffusione di informazioni legate ad un uso corretto della tecnologia digitale.

Saranno utilizzati firewall, filtri e software che impediscono i collegamenti ai siti web per adulti (black list) o a siti non inerenti alle attività scolastiche.

In questi anni, i docenti hanno effettuato e continueranno a svolgere attività di formazione/informazione in classe e in orario extrascolastico avvalendosi della collaborazione di

esperti esterni e di associazioni del territorio per sensibilizzare gli alunni e le famiglie, avvalendosi di materiali di supporto, fra cui quelli messi a disposizione da “Generazioni Connesse”.

Rilevazione

La collaborazione scuola – famiglia - extrascuola è importante al fine di promuovere un utilizzo consapevole e corretto dei media e quindi oltre a condividere informazioni sulla sicurezza in rete e sui potenziali pericoli è necessario anche informare circa possibili strategie di intervento qualora si rilevassero abusi e/o infrazioni.

<u>Cosa segnalare</u>	Comportamenti inconsueti e/o inadeguati degli alunni.
	Fatti riferiti dagli alunni e/o dalle famiglie ai docenti
	Contenuti pericolosi inviati/ricevuti a/ da altri. messi/scaricati in rete dagli alunni

Il docente deve segnalare comportamenti inconsueti e/o inadeguati da parte degli alunni nei confronti dei compagni o di altri e valutare l'accaduto.

I fatti accaduti possono essere riferiti liberamente dagli alunni o su richiesta diretta del docente.

Possono essere segnalati contenuti pericolosi inviati/ricevuti a/ da altri. messi/scaricati in rete dagli alunni che comprovano l'utilizzo scorretto o criminoso degli strumenti digitali riguardanti:

- la **privacy** (dati personali, foto e video pubblicati contro la propria volontà, ecc. ...);
- la **aggressività** e la **violenza** (commenti offensivi, messaggi minacciosi, contenuti razzisti, immagini o video umilianti, informazioni false, ecc. ...);
- la **sessualità** (messaggi molesti, foto o video pornografici o pedopornografici, conversazioni private riguardanti la sessualità, ecc. ...).

Come segnalare: quali strumenti e a chi

Conservare la prova della condotta incauta, scorretta o dell'abuso rilevata sugli strumenti digitali dell'Istituto o sui telefoni cellulari è utile per far conoscere l'accaduto, in base alla gravità, ai genitori degli alunni, al Dirigente scolastico e per condotte criminose alle autorità competenti.

Qualora non si disponga di prove, ma solo della testimonianza dell'alunno o di più persone che hanno partecipato o subito l'accaduto, le notizie raccolte vengono anche queste comunicate dai docenti alle famiglie, al Dirigente scolastico e per condotte criminose alle autorità competenti.

I docenti, in base alla gravità del fatto, decideranno gli strumenti da utilizzare per la segnalazione.

<u>Strumenti da utilizzare</u>	<i>Annotazione del comportamento sul registro e comunicazione scritta ai genitori</i>
	<i>Convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti</i>
	<i>Diario di bordo</i>
	<i>Relazione scritta al Dirigente scolastico</i>

La legge rimette ai genitori dell'alunno la scelta di richiedere l'ammonizione del colpevole attraverso la querela, per quanto riguarda i reati meno gravi.

Per i reati più gravi, i docenti hanno l'obbligo di allertare le autorità competenti e di presentare la denuncia qualora se ne avvisino gli estremi di reato.

Nella denuncia dovrà essere esplicitato:

- ✓ il fatto e il giorno dell'acquisizione del fatto;
- ✓ le fonti di prova;
- ✓ le generalità e il domicilio della persona a cui è attribuito il reato;
- ✓ la persona offesa;
- ✓ i testimoni.

Il Dirigente scolastico, l'equipe pedagogica e/o il Consiglio di classe ha la possibilità di sostituire le sanzioni disciplinari più severe con altri provvedimenti, comprendenti la collaborazione ai servizi interni della scuola (cooperazioni di pulizia e ripristino degli arredi dei locali scolastici o riordino della biblioteca e/o dei laboratori) o altre attività a scopo sociale (ricerche e/o attività di studio ed approfondimento coerenti con l'infrazione commessa) che possono utilmente costituire un rimedio ed un monito.

<u>A chi rivolgersi per chiedere aiuto</u>	<i>Ai genitori</i>
	<i>Al Dirigente Scolastico</i>
	<i>Al Referente del bullismo e del cyberbullismo</i>
	<i>Ai docenti</i>

	Alla Polizia postale
	Alla Chat di Telefono azzurro
	Alla helpline di Generazione Connesse, al numero gratuito 1.96.96.
	A Save the Children

Gestione dei casi

Definizione delle azioni da intraprendere a seconda della specifica del caso.

<i>Cosa segnalare</i>	<i>Come gestire la segnalazione</i>
<i>Uso scorretto di Internet, dei social network e violazione della privacy</i>	Se vengono pubblicati dati personali o materiale scolastico su siti o blog personali che consentono di risalire alle generalità degli alunni, bisogna informare gli insegnanti , il Dirigente, il Referente del bullismo e del cyberbullismo, l'Animatore digitale/ Team digitale che aiutano gli alunni ad evitare che questo comportamento scorretto degeneri e diventi pericoloso.
<i>Bullismo e cyberbullismo</i>	I comportamenti definibili "bullismo" possono esprimersi nelle forme più varie e sono costanti e ripetitivi e nel caso di cyber - bullismo le molestie sono attuate attraverso strumenti tecnologici. Gli interventi sono gestiti dal team docenti in collaborazione con le famiglie attraverso percorsi di mediazione volti alla gestione positiva del conflitto. I docenti, inoltre, attraverso il dialogo aiutano i ragazzi a capire l'importanza di chiedere aiuto, di non diffondere ulteriori notizie online, di essere solidali con i compagni in difficoltà e capire che il bullismo e il cyber-bullismo sono reati punibili dalla legge.
<i>Adescamento online/grooming</i>	I docenti attraverso il dialogo aiutano gli alunni a supportare la vittima, anche con attività di circle time.

<i>Sexting, pornografia e sessualità online</i>	I docenti propongono delle riflessioni sulle relazioni online e propongono attività riguardanti l'affettività e la sessualità. Informano gli alunni che la diffusione di materiale pedopornografico è considerato reato ed è punibile dalla legge italiana. La scuola, inoltre, lavora insieme ad altre figure professionali e alle famiglie, scambiando informazioni e favorendo le occasioni di confronto e di dialogo.
---	---

Procedure operative per la gestione delle infrazioni alla Policy. (Allegato 1)

Le segnalazioni di un uso improprio di Internet sono trattate dal responsabile dell'E-Safety.

- Le denunce di abuso personale devono essere riferite al Dirigente scolastico.
- Gli alunni e i genitori devono essere informati delle procedure di segnalazione.
- Eventuali casi gravi di infrazione alla Policy verranno comunicati alle forze dell'ordine e ai servizi del territorio al fine di stabilire procedure illegali

Procedure operative per la protezione dei dati personali. (Allegato 2)

In ottemperanza al codice sulla privacy (Decreto Legislativo n. 196/2003, codice in materia di protezione dei dati personali) tutti i dati personali dei componenti della comunità scolastica devono:

- ✓ essere trattati in modo lecito.
- ✓ Essere raccolti e registrati per scopi specifici, espliciti e legittimi.
- ✓ Essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati

L'Istituto comprensivo deve chiedere obbligatoriamente ai genitori degli alunni il permesso prima di scattare foto o di girare video ai propri figli, attraverso la compilazione dell'allegato 2.

Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazione. (Allegato 3)

Per la rilevazione, il monitoraggio e la gestione delle segnalazione saranno attuate le seguenti procedure:

- ✓ Installazione di un server per il controllo degli account e di software di protezione per il monitoraggio dell'utilizzo di Internet.
- ✓ Creazione di "alert" per constatare se i siti web visitati sono coerenti con la E - Policy d'Istituto;
- ✓ Compilazione di un "Diario di bordo" della scuola nel quale riportare le situazioni problematiche online segnalate. (modello proposto da "Generazioni connesse").

Procedure operative per la gestione dei casi

Procedura operativa in caso di pericolo online:

- ✓ ascoltare e capire le problematiche dell'alunno, emerse dall'utilizzo della Rete.

- ✓ coinvolgere i genitori, rispettando i diritti dell'alunno.
- ✓ informare il Referente per il bullismo e cyberbullismo, il referente dell'E-Safety e gli operatori scolastici.
- ✓ in caso di gravi abusi, informare le autorità competenti.
- ✓ rimuovere i contenuti pericolosi online.
- ✓ invitare i compagni a supportare l'alunno in difficoltà.
- ✓ deresponsabilizzare la vittima.
- ✓ proporre discussioni di gruppo e coinvolgere la comunità scolastica in percorsi di prevenzione.
- ✓ compilare il "Diario di bordo" per poter tenere traccia di ciò che è avvenuto rispetto ai comportamenti degli alunni online e di come è stato gestito il problema.

LINEE GUIDA PER ALUNNI

- Non comunicare mai a nessuno la tua password e periodicamente cambiala, usando numeri, lettere 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 su un BLOG la fotografia di qualcuno, chiedi sempre il permesso;
- 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 connessi 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;
- Blocca i Bulli: molti Blog e siti social network ti permettono di segnalare i cyberbulli;
- Conserva le comunicazioni offensive, ti potrebbero essere utili per dimostrare quanto ti è accaduto;
- Se ricevi materiale offensivo (e-mail, 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 è consigliabile inviare mail personali, perciò rivolgeti sempre al tuo insegnante prima di inviare messaggi di classe o ai tuoi genitori prima di inviare messaggi da casa;
- Non scaricare (download) o copiare materiale da Internet senza il permesso del tuo insegnante o dei tuoi genitori;
- 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 sui computer o sul server della scuola, lo spazio è limitato e di uso comune;
- Salvate sempre i vostri lavori (file) in cartelle personali e/o di classe e non sul desktop o nella cartella del programma in uso. Sarà cura di chi mantiene il corretto funzionamento delle macchine cancellare file di lavoro sparsi per la macchina e al di fuori delle cartelle personali;
- Discutete con gli alunni della policy e-safety della scuola, dell' 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 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, Servizi Sociali per la fruizione di servizi socio-educativi comunali, ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare);
- Chiedete/suggerite di cancellare il materiale offensivo, bloccare o ignorare particolari mittenti, uscire da gruppi non idonei, cambiare indirizzo e-mail, ecc... ;
- 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 il Dirigente Scolastico, l'Animatore digitale, il Referente per il bullismo per un eventuale denuncia all'autorità giudiziaria o agli organi di Polizia.

CONSIGLI AI GENITORI PER UN USO RESPONSABILE DI INTERNET A CASA

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, di approfondimenti disciplinare...
- Partecipa alle esperienze on-line: naviga insieme a tuo figlio, discuti gli eventuali problemi che si presentano;
- Comunicate elettronicamente con vostro figlio: inviate, frequentemente, E-mail, Instant Message;
- 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 riconoscerne insieme i rischi potenziali.

Allegato 1



MINISTERO DELL' ISTRUZIONE UNIVERSITÀ RICERCA
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
ISTITUTO COMPRENSIVO "MARTIN LUTHER KING"
VIA DEGLI ORAFI n° 30 - 00133 ROMA - DISTRETTO SCOLASTICO XVI
tel.06/2023327/2023663 - fax: 06/2023327 C. M. RMIC85300C
e-mail RMIC85300C@ISTRUZIONE.IT - C.F. 9719797058
sito web: www.icmlking.gov.it



Modulo di richiesta per l'accesso ad internet nella rete di Istituto e per l'utilizzo dei dispositivi elettronici

Al Dirigente Scolastico

Il/La sottoscritto/a _____,
nato/a _____ prov. _____ residente a _____
_____ in via/piazza _____, n. _____
_____ CAP _____ e – mail _____
in qualità di genitore dell'alunno _____, Iscritto/a alla
classe _____ sez. _____ plesso _____

Dichiara

Di essere consapevole delle implicazioni di responsabilità personali derivanti dall'accesso alla Rete Internet e dell'uso del cellulare e degli eventuali abusi.

In particolare si impegna a che il/la figlio/a:

- ❖ non scarichi/duplichi/distribuisca software o altri contenuti protetti da diritto d'autore;
- ❖ non acceda a siti o risorse dal contenuto illegale o non consono alle regole di comportamento dettate dal carattere istituzionale ed educativo dell'Istituto;
- ❖ non diffonda virus o altri software malevoli all'interno della rete;
- ❖ non utilizzi il cellulare o altri dispositivi elettronici personali a scuola se non autorizzato dal docente;
- ❖ partecipi agli interventi educativi dell'Istituto sulle modalità di utilizzo sicuro e consentito dei dispositivi elettronici e di Internet.

Data, _____

Firma _____



MINISTERO DELL' ISTRUZIONE UNIVERSITÀ RICERCA
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
ISTITUTO COMPrensIVO "MARTIN LUTHER KING"
VIA DEGLI ORAFI n° 30 - 00133 ROMA - DISTRETTO SCOLASTICO XVI
tel.06/2023327/2023663 - fax 06/2023327 C. M. RMIC85300C
e-mail RMIC85300C@ISTRUZIONE.IT C.F. 9719797058
sito web: www.icmlking.gov.it



TUTELA DELLA PRIVACY DEI MINORI
DICHIARAZIONE LIBERATORIA PER FOTOGRAFIE E RIPRESE VIDEO
(D.Lgs. 196/2003 – Codice in materia di protezione dei dati personali)

Il/La sottoscritto/a _____,
nato/a _____ prov. _____ residente a _____
in via/piazza _____, n. _____
CAP _____ e – mail _____
in qualità di genitore dell' alunno _____, Iscritto/a alla
classe _____ sez. _____ plesso _____

AUTORIZZA
 NON AUTORIZZA

La scuola a riprendere e/o a far riprendere, con apparecchiature fotografiche e audiovisive, il/la proprio/a figlio/a da solo o con i compagni: in occasione delle attività didattiche, durante le visite e i viaggi di istruzione, in tutti gli eventi connessi con il piano dell'offerta formativa dell'Istituto Comprensivo.

PRENDE ATTO E ACCONSENTE

Che le riprese video e le fotografie verranno utilizzate esclusivamente per scopi didattici: per pubblicizzare le attività dell'Istituto, quali partecipazioni a concorsi, in occasione di esposizioni e/o mostre didattiche, durante le feste all'interno dell'Istituto o nel territorio.

Che l'alunno non autorizzato sarà temporaneamente esentato dall'attività nel momento della ripresa.

SOLLEVA

L'Istituto da ogni responsabilità per un eventuale uso non autorizzato delle immagini da parte di terzi non citati. Tale autorizzazione si intende gratuita e valida per tutto il periodo di permanenza nell'Istituto, salvo diversa disposizione.

DICHIARA

Di essere a conoscenza del divieto di divulgazione di immagini o filmati altrui senza il consenso e, pertanto, del divieto alla pubblicazione e condivisione sul web, sui social network o altrove, di foto e video, seppur personali, che ritraggano anche altri bambini.

Data, _____

Firma _____

Allegato 3

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?		

Protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi.

L'Istituto non ha siglato protocolli con le forze dell'ordine o con i servizi messi a disposizione nel territorio per la gestione condivisa dei casi, ma ha concordato e organizzato ricorrenti forme di collaborazione nella prevenzione e contrasto del bullismo e del cyberbullismo con la Polizia dello Stato e con associazioni del settore.

Regolamento di accesso e di uso dei laboratori multimediali. (allegato 4)

Si allega il Regolamento vigente nel nostro Istituto riguardante l'accesso e l'utilizzo dei laboratori multimediali.

