SCUOLA SECONDARIA DI 1° GRADO
"RICCARDO MONTERISI"
BISCEGLIE

E-Safety Policy

1. Introduzione

Negli ultimi anni, il nostro Istituto ha visto crescere l'uso delle tecnologie informatiche nella gestione generale della Scuola e nella didattica. Oggi è normale che a scuola ci si connetta ad Internet, non solo per svolgere funzioni amministrative-gestionali, ma anche per dare un respiro più ampio alle esperienze formative degli studenti attraverso l'uso di laboratori, tablet e cellulari e rendere l'esperienza a scuola più vicina al mondo degli studenti *nativi digitali*.

Internet è certamente molto utile, però può essere anche una potenziale fonte di rischi, tanto maggiori quanto meno si conoscono i modi legittimi di utilizzo e si abbia scarsa consapevolezza delle funzioni della rete. "Il confine tra uso improprio e uso intenzionalmente malevolo della tecnologia è sottile […] ed è in questa zona di confine che si sviluppano quei fenomeni che sempre più frequentemente affliggono i giovani e che spesso emergono nel contesto scolastico." (*LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrato al bullismo e al cyberbullismo,* aprile 2015)

Alla luce di queste considerazioni, la progettualità relativa alla tutela della sicurezza informatica nel nostro Isituto non può prescindere dal contrasto al cyberbullismo e, pertanto, opera su due livelli paralleli: da un lato la conoscenza dei contenuti tecnologici e la comprensione critica dei mezzi di comunicazione, dall'altro la creazione di un ambiente di apprendimento accogliente ed inclusivo che favorisca l'adozione di comportamenti corretti anche in rete, spesso vissuta come un'estensione *virtuale* dell'esperienza quotidiana *reale* (vedi PTOF, sezione 2.6.1 e sezione 3).

Tale progettualità vede coinvolto tutto il personale della scuola, gli studenti e le famiglie.

In particolare, "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 […] La scuola è chiamata ad adottare misure atte a prevenire e contrastare ogni forma di violenza e prevaricazione; la famiglia è chiamata a collaborare, non solo educando i propri figli ma anche vigilando sui loro comportamenti." (*LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrato al bullismo e al cyberbullismo,* aprile 2015).

Scopo della Policy

Il presente documento, da un punto di vista legislativo e amministrativo, è ispirato e promosso da direttive del Ministero dell'Istruzione a livello nazionale e regionale e fa costante riferimento alle norme legislative specifiche del settore.

Attraverso tale documento, l'Istituto si propone di:

- regolamentare l'utilizzo delle TIC di cui si avvalgono i membri della comunità scolstica;
- impostare chiare aspettative di comportamento e/o codici di condotta rilevanti per un uso responsabile di Internet a scopo didattico, personale o ricreativo;
- affrontare gli abusi online (come il cyerbullismo);
- garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che il comportamento illecito o pericoloso è inaccettabile e che saranno intraprese le opportune azioni disciplinari e giudiziarie.

A tale scopo vengono definite:

- le norme relative all'accesso alle postazioni in rete della scuola da parte dei diversi soggetti operanti nell'Istituto (docenti, ATA, studenti, eventuali soggetti esterni alla scuola);
- le norme riguardanti l'accesso ai servizi resi disponibili sui computer in rete da parte dei diversi soggetti operanti nell'Istituto;
- le regole riguardanti le garanzie a tutela della privacy nell'uso degli strumenti tecnologici d'Istituto;
- le regole riguardanti l'utilizzo degli strumenti personali (cellulari, tablet, ecc.).

Ruoli e Responsabilità

Al fine di garantire la sicurezza delle TIC, la scuola attua diverse strategie.

Il Dirigente Scolastico si riserva, sentiti i responsabili, di limitare l'accesso e l'uso della rete interna (Intranet) ed esterna (Internet) secondo i normali canali di protezione presenti nei sistemi operativi.

La scuola promuove e adatta ogni accorgimento per evitare comportamenti contrari alle norme del Regolamento d'Istituto, quali:

- scaricare file video-musicali protetti da copyright;
- visitare siti non necessari ad una normale attività didattica;
- 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.

Nello specifico tutti gli utenti sono consapevoli che:

- il sistema informatico è periodicamente controllato dai responsabili (DSGA e personale responsabile su nomina del Dirigente Scolastico);
- la scuola può controllare periodicamente i file utilizzati, i file temporanei e i siti visitati da ogni dispositivo;
- la scuola archivia i tracciati del traffico Internet;
- è vietato installare e scaricare da Internet software non autorizzati;

- al termine di ogni collegamento la connessione deve essere chiusa;
- verifiche antivirus sono condotte periodicamente sui computer e sulle unità di memorizzazione di rete dai responsabili;
- l'utilizzo di CD, chiavi USB e floppy personali 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.

RUOLO	RESPONSABILITÀ
Dirigente Scolastico	▪ garantire che la scuola utilizzi un Internet Service filtrato approvato, conforme ai requisiti di legge vigenti ; ▪ assicurare che il personale riceva una formazione adeguata per svolgere i ruoli di sicurezza on-line e per la formazione di altri colleghi; ▪ stabilire contatti con le autorità locali e le agenzie competenti, finalizzati ad azioni di prevenzione e/o di supporto alla gestione dei casi rilevati; ▪ ricevere relazioni di monitoraggio periodiche della sicurezza online da parte del responsabile.
Direttore Servizi Generali Amministrativi	▪ assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi 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.
Responsabili della sicurezza online **(DSGA e personale responsabile su nomina del DS)** **Docente referente per il bullismo/cyberbullismo**	▪ promuovere la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica; ▪ garantire che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente per la sicurezza online; ▪ controllare la condivisione di dati personali; ▪ controllare l'accesso a materiali illegali / inadeguati; ▪ effettuare il monitoraggio delle segnalazioni e seguire la gestione dei casi.
Animatore Digitale e Team per l'innovazione	▪ stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornisce 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 nell'intera comunità; ▪ 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 (istruzione e formazione); ▪ coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".
Docenti	▪ discutere con gli alunni delle norme adottate dalla scuola e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di Internet; ▪ dare chiare indicazioni su come si utilizza Internet, ed eventualmente anche la posta elettronica, e informare gli Studenti che le navigazioni sono monitorate; ▪ trattare tematiche legate alla sicurezza online nelle progettazioni disciplinari; ▪ supervisionare e guidare gli alunni quando sono impegnati in attività in cui sia previsto l'uso della tecnologia on-line; ▪ garantire agli alunni l'acquisizione delle competenze sociali e civiche e di quelle digitali, al fine di favorire una maggiore coscienza critica nel processo di alfabetizzazione informatica, in modo che per tutti Internet sia una risorsa e un diritto e non un pericolo.
Personale scolastico	▪ 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; ▪ segnalare qualsiasi abuso sospetto o problema ai responsabili della sicurezza online.
Studenti	▪ essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti; ▪ 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 sia a scuola sia a casa; ▪ adottare condotte rispettose degli altri anche quando si comunica in rete; ▪ conoscere e capire la politica relativa all'uso dei telefoni cellulari, fotocamere digitali e dispositivi portatili; ▪ esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

Genitori	▪ sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica; ▪ seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di internet; ▪ concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o 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.

Condivisione e comunicazione della Policy all'intera comunità scolastica

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

- condivisione con la comunità scolastica attraverso gli organi collegiali;
- pubblicazione della E-Safety Policy sul sito della scuola;
- condivisione con gli studenti e i genitori, all'inizio del primo anno, tramite il Patto di Corresponsabilità, che sarà sottoscritto dalle famiglie e rilasciato alle stesse.

Monitoraggio dell'implementazione della Policy e suo aggiornamento

La E-Safety Policy si inserisce all'interno di altre politiche scolastiche, quali, *in primis* la protezione dei minori, la prevenzione del bullismo e la salvaguardia degli alunni a scuola.

La E-Safety Policy sarà riesaminata sulla base dei dati rilevati alla fine di ciascun anno scolastico qualora si registrino variazioni significative del livello di rischio complessivo all'interno dell'Istituto o intervengano cambiamenti rilevanti riguardo le tecnologie in uso all'interno della scuola.

Tutte le modifiche della Policy saranno discusse nell'ambito degli organi competenti, per una condivisione unanime.

Integrazione della Policy con Regolamenti esistenti

La Policy è coerente con quanto stabilito dalla Legge (Statuto delle studentesse e degli studenti della scuola secondaria DPR 24 giugno 1998 n. 249 modificato dal DPR 21 novembre 2007 n. 235; Legge 29 maggio 2017 n. 71 "Disposizioni a tute dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo"; Legge 31 dicembre 1996 n. 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali"), dal Regolamento d'Istituto e dal Patto di Corresponsabilità.

2. Formazione e Curricolo

Curricolo sulle competenze digitali per gli studenti

Il nostro istituto, nell'ambito della propria offerta formativa, ha attivato da diversi anni percorsi curricolari ed extracurricolari finalizzati allo sviluppo delle **competenze chiave di cittadinanza**. In quest'ottica le azioni di prevenzione e contrasto dei fenomeni di bullismo e cyberbullismo sono inserite in un quadro strategico di interventi strutturati e coerenti con l'articolazione del curricolo di istituto, che tra le finalità generali si propone di promuovere l'acquisizione di conoscenze e competenze necessarie per l'esercizio di una piena cittadinanza e di fornire gli strumenti per operare scelte autonome consapevoli, improntate alla comprensione degli altri e al rispetto della diversità.

La **competenza digitale** viene considerata in una dimensione trasversale che riguarda tutte le discipline, in quanto, per sua natura richiede non solo il possesso delle abilità tecniche di base, ma anche la maturazione dello spirito critico, il reperimento, il confronto, la conservazione e lo scambio delle informazioni; la valutazione dell'affidabilità delle fonti; la partecipazione a reti collaborative.

Per quanto riguarda la formazione degli studenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali, il nostro istituto ha messo in campo attività specifiche integrate in alcuni moduli didattici curricolari, sui seguenti temi: educazione al rispetto e alla cittadinanza digitale. Inoltre vengono regolarmente organizzati incontri con le forze dell'ordine con riferimento ai temi della cittadinanza digitale, con particolare attenzione alla prevenzione dai rischi online.

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

Per quanto riguarda la formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica, il corpo docente possiede conoscenze specifiche sulle TIC (anche derivante da corsi di formazione organizzati dalla scuola) e le utilizza nella didattica. Conosce e utilizza i pacchetti di scrittura, calcolo e presentazioni e li utilizza per produrre materiale didattico di supporto (cartaceo e digitale). Ha la possibilità di utilizzare la LIM a scuola, per l'elaborazione di materiale didattico digitale, destinato ad integrare le presentazioni in classe e approfondire i moduli tematici.

Negli ultimi due anni, sono stati sostenuti corsi di aggiornamento in merito all'utilizzo delle TIC nella didattica, con una ricaduta positiva dal momento che all'acquisizione delle competenze è seguito il loro utilizzo nella didattica.

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

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.

All'interno della Bacheca docenti online all'interno del sito della scuola sono stati condivisi materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di internet, materiali informativi sulla sicurezza in internet per l'approfondimento personale, per le attività con gli studenti e gli incontri con i genitori, costituiti da guide in pdf, video, manuali a fumetti, link a siti specializzati e contributi della Polizia di Stato, dell'Arma dei Carabinieri, di Telefono Azzurro, dal sito "Generazioni connesse", ecc.

Il corpo docente partecipa sistematicamente all'individuazione delle azioni prioritarie del PNSD, da implementare nella scuola, supportando uno o più docenti di riferimento.

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.

Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo.

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

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

Accesso a internet: filtri, antivirus e sulla navigazione.

L'infrastruttura e la strumentazione TIC dell'Istituto sono un patrimonio di tutti, esse vanno utilizzate nel rispetto delle norme relative all'utilizzo dei laboratori multimediali. I danni causati alle attrezzature saranno a carico di chiunque disattenda il suddetto Regolamento. L'accesso ad infrastrutture e strumentazione TIC utilizzabili per la didattica è riservato ai docenti e agli alunni ed è limitato al perseguimento di scopi formativi. I docenti devono formare i propri alunni al rispetto del suddetto Regolamento, per gli aspetti di loro pertinenza. La scuola deve considerare l'ambiente online alla stregua dell'ambiente fisico, e valutarne tutti gli aspetti legati alla sicurezza nel momento in cui permette l'accesso alla rete tramite i collegamenti scolastici.

L'accesso a Internet avviene attualmente nel nostro istituto tramite WIFI protetto da password. Il suo utilizzo è ovviamente legato alle esigenze di programmazione didattica e all'espletamento delle pratiche burocratiche. La Scuola promuove e adotta ogni accorgimento per evitare comportamenti contrari alle norme di sicurezza informatica, come: scaricare file video protetti da copyright; visitare siti non necessari ad una normale attività didattica; alterare i parametri di protezione dei computer in uso; utilizzare la rete per interessi privati e personali che esulano dalla didattica; utilizzare le proprie pen drive, non rispettare le leggi sui diritti d'autore; navigare su siti non raccomandabili.

Nella pratica didattica, il docente è il primo soggetto che favorisce l'uso corretto della rete, guidando gli studenti nelle attività online, stabilendo obiettivi chiari di ricerca, insegnando le strategie appropriate nella definizione e gestione della risorsa informatica.

Gli alunni accedono alla rete, sotto precisa responsabilità e controllo del docente, dai terminali presenti nei laboratori, mentre l'uso della rete nelle singole classi non è a loro consentito. Non è inoltre loro consentito modificare a qualsiasi titolo le impostazioni dei computer (salvaschermo, sfondo, colori, risoluzioni, suoni, pagina iniziale di Internet, account di posta elettronica…).

Tutti i Pc della nostra Scuola (desktop o portatili), privi di webcam, sono dotati di programmi antivirus (del tipo open-source) e muniti di firewall attivo.

Gestione accessi (password, backup, ecc.)

I computer portatili presenti nelle aule dove c'è la LIM non richiedono una password di accesso per l'accensione perché custoditi all'interno di un armadio di sicurezza chiuso a chiave. Ogni docente è quindi tenuto ad un controllo della strumentazione in aula poiché l'uso del dispositivo è permesso agli alunni solo su autorizzazione dell'insegnante. Ogni docente accede al registro elettronico attraverso una password personale, da custodire diligentemente, che non può essere comunicata a terzi, né agli alunni.

E-mail

L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. L'eventuale invio o ricevimento di posta a scopi didattici avviene solo su autorizzazione del Dirigente scolastico e operativamente è svolto dall'assistente amministrativo addetto. La posta elettronica è protetta da antivirus e quella certificata anche dall'antispam.

Blog e sito web della scuola, social network, protezione dei dati personali

L'Istituto dispone di un proprio spazio web e di un proprio dominio: www.scuolamediamonterisi.gov.it

L'Istituto gestisce un proprio sito web nello spazio di proprietà secondo le modalità di seguito esplicitate:

- la gestione delle pagine del sito della scuola è curata da un gruppo di docenti, a garanzia che i contenuti pubblicati sul sito siano chiari e appropriati;
- per i documenti che si trovano sul sito viene 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 pubblicherà fotografie degli alunni esclusivamente previo consenso dei loro genitori. Le fotografie degli studenti per il sito della scuola saranno selezionate in modo tale che solo gruppi di alunni siano ritratti in attività didattiche a scopi documentativi;
- la scuola rende consultabili all'interno del proprio sito web i seguenti contenuti: Piano triennale dell'offerta formativa, Regolamento d'Istituto, Patto di corresponsabilità e altri documenti allegati al PTOF; informazioni generali sull'Istituto, informazioni sui progetti attivati, informazioni sull'amministrazione, Albo d'Istituto, elenchi libri di testo, sezione Area riservata docenti;
- l'Istituto si impegna a mantenere efficienti questi servizi, a migliorarli e estenderli nell'ottica di aumentare la qualità del servizio offerto.

4. Utilizzo della strumentazione personale e della strumentazione ICT della scuola

Studenti

Come da Regolamento d'Istituto agli studenti è consentito l'uso del cellulare o dei tablet all'interno della scuola esclusivamente alla presenza del docente e per ragioni prettamente didattiche. Nell'utilizzo dei computer messi a disposizione dalla scuola e della propria strumentazione personale gli studenti devono attenersi alle seguenti indicazioni:

- non utilizzare giochi né in locale, né in rete;
- salvare sempre i lavori propri (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;
- mantenere segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della scuola;
- non inviare a nessuno fotografie personali o di propri amici;
- chiedere sempre al Docente il permesso di scaricare documenti da Internet;
- chiedere sempre l'autorizzazione al Docente prima di iscriversi a qualche concorso o prima di riferire l'indirizzo della propria scuola;
- riferire immediatamente al Docente nel caso in cui qualcuno invii immagini inappropriate od offensive. Non rispondere, in ogni caso, al predetto invio;
- riferire al Docente in caso di reperimento di immagini inappropriate od offensive durante la navigazione su Internet;
- riferire al Docente, o comunque ad un adulto, qualora qualcuno su Internet chieda un incontro di persona;
- ricordarsi che le persone che si "incontrano" nella Rete sono degli estranei e non sempre sono quello che dicono di essere;
- non è consigliabile inviare mail personali, perciò rivolgersi sempre all'insegnante prima di inviare messaggi di classe;
- non caricare o copiare materiale da Internet senza il permesso dell'insegnante o del responsabile di laboratorio.

Docenti e personale della scuola

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

In particolare, per quanto riguarda i docenti *"il divieto di utilizzare telefoni cellulari durante lo svolgimento di attività di insegnamento - apprendimento, del resto, opera anche nei confronti del personale docente (cfr.*

Circolare n. 362 del 25 agosto 1998), in considerazione dei doveri derivanti dal CCNL vigente e dalla necessità di assicurare all'interno della comunità scolastica le migliori condizioni per uno svolgimento sereno ed efficace delle attività didattiche, unitamente all'esigenza educativa di offrire ai discenti un modello di riferimento esemplare da parte degli adulti" (Circolare Ministeriale n.30 del 15 marzo 2007).

Nell'utilizzo dei computer messi a disposizione dalla scuola, Docenti e personale ATA devono attenersi alle seguenti indicazioni:

- evitare di lasciare le e-mail o file personali sui computer o sul server della scuola;
- salvare sempre i lavori propri (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;
- ricordare 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);
- tutti gli utilizzatori di computer, siano essi docenti, personale ATA e studenti, non devono lasciare a lungo sui computer in uso, file di grosse dimensioni e/o non più utilizzati per molto tempo onde evitare di occupare spazio.

5. Prevenzione, rilevazione e gestione dei casi

Attraverso percorsi formativi specifici il nostro Istituto promuove lo sviluppo di competenze digitali e civiche necessarie per un utilizzo consapevole e responsabile delle Nuove Tecnologie. Educare ai *nuovi media*, ai *social media* e alla *società dell'informazione* in genere, significa mettere gli alunni nella condizione di apprezzare le opportunità positive che la Rete mette a disposizione, ma al tempo stesso di conoscere i rischi legati ad un uso non consapevole delle risorse digitali. Coerentemente con questa finalità educativa la scuola mette in atto strategie di carattere preventivo attraverso lo sviluppo di competenze relazionali, sociali e civiche.

Tuttavia di fronte all'emergere, nel contesto scolastico, di un evento problematico legato ai rischi online è opportuno mettere in atto procedure chiare e standardizzate di intervento, al fine di consolidare una prassi comune e condivisa per la rilevazione, la segnalazione e la gestione dei casi.

I rischi effettivi che si possono correre a scuola nell'utilizzo delle TIC da parte degli alunni derivano da un uso non corretto del telefono cellulare personale o dello smartphone o dei PC della scuola collegati alla rete.

Eludendo la sorveglianza degli insegnanti, attraverso i telefoni cellulari o gli smartphone, dotati di particolari applicazioni e di collegamento a internet, gli alunni potrebbero interagire con l'esterno o con altri alunni tramite telefonate o messaggi, ma anche scaricare e spedire foto personali o intime, proprie o di altri, video con contenuti indecenti o violenti, accedere a internet e a siti non adatti ai minori, ascoltare musica e giocare con i videogiochi non consigliati ai minori, leggere la posta elettronica e comunicare o chattare con sconosciuti, inviare o ricevere messaggi molesti e minacciosi. Eludendo sempre la vigilanza degli insegnanti, gli alunni potrebbero correre gli stessi rischi a scuola anche con l'utilizzo dei PC del laboratorio informatico e con un accesso non controllato a internet.

Le procedure standardizzate costituiscono strumenti operativi di supporto e accompagnamento di tutti gli operatori scolastici (Dirigente, docenti, personale ATA) che consentono di gestire le diverse situazioni in maniera efficace e tempestiva. È bene, comunque, tener presente che ogni caso va considerato nel contesto specifico, valutando di volta in volta il livello di gravità che lo caratterizza e considerando sempre come prioritari l'interesse del minore, il suo diritto alla cura, alla protezione e alla privacy.

Procedure operative per la gestione delle infrazioni alla Policy

PROCEDURE OPERATIVE PER LA RILEVAZIONE, IL MONITORAGGIO E LA GESTIONE DELLE SEGNALAZIONI		
Raccolta informazioni	**Iniziative con gli adulti**	**Iniziative con la classe**
Si **sospetta** che stia accadendo uno o più alunni siano coinvolti in una situazione di rischio online.	Dialogare con i colleghi: confrontarsi per condividere preoccupazioni ed acquisire informazioni.	Parlare dei rischi connessi ad uno non responsabile delle Nuove Tecnologie e delle loro conseguenze.
	Monitorare la situazione ascoltando quanto riferito da docenti, collaboratori e alunni, anche in situazioni informali.	Stabilire un clima di fiducia che faciliti la condivisione di informazioni sull'accaduto. Proporre attività in classe sull'empatia e sul riconoscimento delle emozioni (proprie e altrui).
	Condividere le preoccupazioni con il/la referente per il cyberbullismo. Valutare con lui/lei le possibili strategie di intervento.	Monitorare la situazione e far emergere il problema in modo evidente, anche attraverso modalità laboratoriali. Se ancora non ci sono evidenze, lavorare sul clima all'interno della classe e continuare a monitorare la situazione.
	Valutare la gravità del rischio per metterne eventualmente al corrente il Dirigente Scolastico	Informare gli alunni su ciò che dice la legge italiana sul cyberbullismo e sull'utilizzo non corretto della Rete.
	Raccogliere informazioni per conoscere il livello di diffusione dell'episodio a livello di Istituto	Suggerire di chiedere aiuto a persone competenti per situazioni di questo tipo.
Promuovere per l'intera comunità scolastica percorsi di prevenzione dei comportamenti a rischio online		

PROCEDURE OPERATIVE PER LA GESTIONE DEI CASI		
Raccolta informazioni	**Iniziative con gli adulti**	**Iniziative con la classe**
Si **ha evidenza** che uno o più alunni sono coinvolti in una situazione di rischio online.	Condividere con il referente per il cyberbullismo (e/o il referente indicato nell'e-policy). Valutare con lui/loro le possibili strategie di intervento.	Capire il livello di diffusione dell'episodio a livello di Istituto e parlare della necessità di non diffondere ulteriormente online i materiali.
	Avvisare il Dirigente Scolastico	Dialogare con la classe sul cyberbullismo e sulle sue conseguenze (non nominare gli alunni coinvolti). Suggerire di chiedere aiuto per situazioni di questo tipo.
	Richiedere la consulenza di esperti a supporto della gestione della situazione, in base alla gravità.	Prevedere un momento laboratoriale in modo da facilitare l'elaborazione della situazione.
	Dialogare con i colleghi/e: confrontarsi per condividere informazioni e strategie.	Dialogare con la classe. A seconda della situazione trova il modo di supportare la vittima e di responsabilizzare i compagni, rispetto al loro ruolo, anche di spettatori, nella situazione.
	Informare i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto). Richiedere, se possibile, la presenza dello psicologo/a, per condividere informazioni e strategie.	
	Informare i genitori di ragazzi/e infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy)	Promuovere per l'intera comunità scolastica percorsi di prevenzione dei comportamenti a rischio online.
	Valutare come coinvolgere gli operatori scolastici su quanto sta accadendo	
	A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnalare alla Polizia Postale: a) contenuto; b) modalità di diffusione Se è opportuno, richiedere un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).	Tenere traccia di quanto successo e delle azioni intraprese: compila il diario di bordo

ALLEGATO 1
MODULO PER LA SEGNALAZIONE E IL MONITORAGGIO DEI CASI DI BULLISMO/CYBERBULLISMO

Nome di chi compila la segnalazione	Ruolo: Data:
Descrizione dell'episodio o del problema □ bullismo □ cyberbullismo	
Soggetti coinvolti	Vittima/e: Classe: 1. 2. 3. Bullo/i: Classe: 1. 2. 3.
Chi ha riferito dell'episodio?	□ la vittima □ un compagno della vittima, nome: □ genitore, nome: □ insegnante, nome: □ altri, specificare:
Atteggiamento del gruppo	Da quanti compagni è sostenuto il bullo? Quanti compagni supportano la vittima o potrebbero farlo?
Gli insegnanti sono intervenuti in qualche modo ?	
La famiglia o altri adulti hanno cercato di intervenire ?	
Chi è stato informato della situazione?	□ coordinatore di classe, in data □ consiglio di classe, in data: □ dirigente scolastico, in data: □ la famiglia della vittima/e, in data: □ la famiglia del bullo/i, in data: □ le forze dell'ordine, in data: □ altri, specificare:
1° Monitoraggio effettuato in data:	Azioni intraprese: La situazione è □ migliorata □ invariata □ peggiorata
2° Monitoraggio effettuato in data:	Azioni intraprese: La situazione è □ migliorata □ invariata □ peggiorata