



ISTITUTO COMPRENSIVO "GAUDENZIO FERRARI"
via Marconi, 9 - 28015 MOMO (NO)
tel. 0321 926134 - fax 0321 925666
e-mail: noic817009@istruzione.it codice fiscale 80010620039



E-Safety Policy a.s. 2017/2018

1. INTRODUZIONE

- Scopo della Policy.
- Ruoli e Responsabilità.
- Condivisione e comunicazione della Policy all'intera comunità scolastica.
- Gestione delle infrazioni alla Policy.
- Monitoraggio dell'implementazione della Policy e suo aggiornamento.
- Integrazione della Policy con Regolamenti esistenti.

2. FORMAZIONE E CURRICOLO

- Curricolo sulle competenze digitali per gli studenti.
- Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica.
- Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Sensibilizzazione delle famiglie.

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

- Accesso ad internet e Gestione accessi.
- E-mail.
- Sito web della scuola
- Social network.
- Protezione dei dati personali.

4. STRUMENTAZIONE PERSONALE

- Studenti
- Docenti e altro personale

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

- Prevenzione
 - Rischi
 - Azioni
- Rilevazione - Come segnalare: quali strumenti e a chi.
- Gestione dei casi.
- Definizione delle azioni da intraprendere a seconda della specificità del caso.

Allegati

- Modulo di segnalazione
- Schema riepilogativo delle situazioni gestite legate a rischi on-line (da "Generazioni Connesse")

1. INTRODUZIONE

1.1 Scopo della Policy

Il nostro Istituto ha visto crescere negli anni l'uso delle tecnologie informatiche nella didattica e nella gestione generale della scuola. Oggi è normale che a scuola ci si connetta ad Internet, sia per svolgere esperienze formative, sia per le funzioni amministrative-gestionali. Internet è 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. Questo vale certamente per il complesso sistema di computer in rete presenti nella scuola: sia riguardo ai tradizionali laboratori, sia riguardo agli uffici amministrativi e più in generale alle aule singole predisposte per il collegamento interno ed esterno. Le norme che seguiranno richiamano gli utenti ad un uso corretto e generalizzato delle infrastrutture di rete (interna ed esterna), il cui uso improprio può generare problemi, da un punto di vista didattico; nonché difficoltà di uso delle macchine, con possibili danni al loro funzionamento e connessi danni di natura economica.

Lo scopo della E-Safety Policy è:

- di stabilire i principi fondamentali tipici di tutti i membri della comunità scolastica per quanto riguarda l'utilizzo di tecnologie,
- di salvaguardare e proteggere i bambini, i ragazzi e lo staff dell'Istituto;
- assistere il personale della scuola a lavorare in modo sicuro e responsabile con altre tecnologie di comunicazione di Internet e monitorare i propri standard e le prassi;
- 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 cyberbullismo, che sono riferimenti incrociati con le altre politiche della scuola;
- 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.

E' dunque importante definire all'interno dell'istituto alcune regole chiare che permettano di lavorare in modo sereno e consentano di usare le tecnologie in modo efficiente e positivo. Questo documento costituisce parte integrante del Regolamento di Istituto e verrà portato a conoscenza dei genitori, degli studenti e di tutto il personale della scuola. Le norme di questo documento valgono per tutti gli spazi e laboratori dell'Istituto. Il personale interno all'Istituto (docenti, ATA e studenti) ed esterno (genitori, tirocinanti, esperti che collaborano con la scuola, ecc.) prende visione del presente documento, che sarà revisionato annualmente. Il presente regolamento, 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.

1.2 Ruoli e responsabilità

Dirigente scolastico	Il Dirigente Scolastico promuove le azioni necessarie per attuare le norme del presente regolamento, controllarne l'attuazione, irrogare le sanzioni, comunicare con enti esterni alla scuola. Per questa attività si avvale anche della consulenza della funzione strumentale ITC e dell'animatore digitale.
DSGA	<p>Nei limiti dei bilanci, pianifica gli interventi tecnici e gli acquisti per garantire l'efficienza e continuità e innovazione della scuola.</p> <p>Garantisce la presenza e l'efficienza del registro elettronico dell'istituto.</p>
ITC dell'istituto	Si occupa di garantire l'efficienza delle infrastrutture informatiche della scuola segnalando alla DSGA e al Dirigente le problematiche hardware e software dei plessi e le esigenze di alunni e docenti.
Docenti	<ul style="list-style-type: none"> • Pongono la massima cura che le password di accesso ai sistemi della scuola (registro elettronico e WiFi) non siano conosciute dagli alunni; • I docenti che portano gli alunni nell'aula informatica illustrano, nel caso in cui gli alunni devono accedere alla rete internet per la loro attività, le regole adottate dalla scuola e gli eventuali problemi che possono verificarsi; • Ricordano agli alunni che la violazione consapevole delle norme adottate dall'Istituto comporta le sanzioni previste nella sezione disciplina alunni del presente regolamento; • Non scaricano file video o musicali protetti da copyright; • Consultano il responsabile ITC prima di scaricare/installare software che ritengono utile. • Si accertano preventivamente che i pendrive USB personali che devono collegare ai PC della scuola siano privi di virus o malware.
Personale scolastico	Vigila, di concerto con i docenti, che gli studenti non utilizzino telefoni cellulari.
Alunni	<p>Gli alunni nelle attività in cui utilizzano i PC della scuola:</p> <ul style="list-style-type: none"> • non devono utilizzare giochi nè in locale nè in rete; • devono riferire all'insegnante in caso di reperimento di immagini inappropriate od offensive durante la navigazione su Internet; • devono chiedere l'autorizzazione al Docente nel caso per l'attività svolta in rete occorra iscriversi e segnalare l'indirizzo della scuola; • devono chiedere al Docente il permesso prima di scaricare documenti dalla rete, e in ogni caso non scaricano file video o musicali protetti da copyright; • Non devono scaricare / installare sui PC della scuola software senza

l'autorizzazione del docente;

- devono chiedere al docente presente in aula il permesso per collegare un loro pendrive USB ai PC della scuola, assicurandosi a casa che siano privi di virus o malware.

Genitori

Devono essere consapevoli che l'accesso alla rete internet dai dispositivi del proprio figlio può essere fonte di pericoli; occorre quindi che vigilino sull'attività online del figlio, e valutino criticamente le richieste di iscrizione ad alcuni social network.

Occorre che collaborino con la scuola nell'educazione ad un uso consapevole dei dispositivi tecnologici.

1.3 Condivisione e comunicazione della Policy all'intera comunità scolastica.

La E-Safety Policy d'istituto si applica a tutte le figure che possono avere accesso alle reti interne della scuola, quali personale docente e studenti, oppure che come genitori ne siano coinvolte nella vigilanza domestica.

All'atto dell'iscrizione o all'inizio dell'anno scolastico la scuola chiede ai genitori degli studenti il consenso all'uso di Internet per il loro figlio e per la pubblicazione dei suoi lavori e delle sue fotografie.

Condivisione e comunicazione della 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 (Consiglio di Istituto, Collegio dei docenti) e pubblicata sul sito web dell'Istituto.

Il personale è consapevole che è sanzionabile una condotta non in linea con il codice di comportamento dei pubblici dipendenti e con la policy d'istituto.

Condivisione della politica di e-safety con i genitori

I genitori saranno informati della policy della scuola e saranno invitati, con metodi che saranno stabiliti, alla collaborazione con la scuola nel perseguire la sicurezza nell'uso di internet. La scuola favorisce una "alfabetizzazione informatica" in modo che, per tutti, Internet possa essere un diritto ed una risorsa.

1.4 Gestione delle infrazioni alla Policy.

Premessa

L'utilizzo della rete interna/esterna (web) avviene all'interno della programmazione didattica e nell'ambito delle esigenze relative alle comunicazioni tra i plessi e la segreteria.

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. L'Istituto regola l'uso dei laboratori indicando norme che consentono di vigilare sull'uso corretto dell'accesso ad Internet.

Disciplina degli alunni

A fronte di violazioni accertate delle regole stabilite dal presente regolamento si assumeranno i provvedimenti disciplinari previsti dal **Regolamento di disciplina**.

La violazione colposa o dolosa accertata delle norme del presente regolamento, oltre all'intervento disciplinare potrà dare luogo alla richiesta di risarcimento delle ore perse per ripristinare il sistema e renderlo nuovamente operante ed affidabile. Rimangono comunque applicabili ulteriori sanzioni disciplinari, eventuali azioni civili per danni, nonché l'eventuale denuncia del reato all'Autorità Giudiziaria. Nel caso di infrazione consapevole da parte dei docenti o del personale non docente, sarà in ogni caso compito del Dirigente Scolastico intervenire per via amministrativa secondo le norme vigenti.

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

Non si può tuttavia escludere che durante la navigazione sui computer dell'Istituto si trovi materiale non appropriato e/o indesiderato.

La scuola non può farsi carico in toto delle responsabilità per il materiale non idoneo trovato o per eventuali conseguenze causate dall'accesso al Web. Per tale ragione, gli utilizzatori devono essere pienamente coscienti dei rischi cui si espongono collegandosi alla rete, riconoscendo ed evitando gli aspetti negativi (*pornografia, violenza, razzismo ...*).

Disciplina del personale scolastico

In caso di violazione colposa o dolosa accertata delle norme del presente regolamento il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

Disciplina dei genitori

E' possibile che alcune condotte dei genitori o loro omissioni di vigilanza possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico.

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

1.5 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 di figure che si occupano dell'informatica nella scuola (referente, animatore digitale, referente ITC, referente commissione PTOF, un rappresentante per ogni plesso della scuola primaria e secondaria di primo grado).

1.6 Integrazione della Policy con Regolamenti esistenti.

Il presente documento va ad integrare i Regolamenti vigenti nell'Istituto e costituisce modello di riferimento per ulteriori regolamenti futuri.

2. FORMAZIONE E CURRICOLO

2.1 Le competenze digitali per gli studenti

“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”.

Competenza digitale significa padroneggiare le abilità e le tecniche di utilizzo delle nuove tecnologie, ma soprattutto utilizzarle con “autonomia e responsabilità” nel rispetto degli altri e sapendone prevenire ed evitare i pericoli. In questo senso, tutti gli insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione.

Il nostro Istituto da alcuni anni si avvale di interventi di Esperti (Polizia di Stato, Carabinieri, Associazione Libera, ecc..) che operano attraverso incontri specifici rivolti agli alunni e aventi come tematica il rispetto della Legalità e l'uso corretto delle nuove tecnologie.

Si sono svolti inoltre alcuni incontri e/o convegni –rivolti rispettivamente sia agli alunni che, in orario serale, alle famiglie- aventi per tema il Cyberbullismo e le conseguenze di un uso scorretto della rete. Si ricordano, fra questi, l'incontro dello scorso maggio con la ex-senatrice Elena Ferrara (promotrice della Legge sul Cyberbullismo), quello di novembre 2017 sulle conseguenze legali connesse ai fenomeni di bullismo e cyberbullismo, e l'ultimo in ordine di tempo lo scorso febbraio 2018 con Paolo Picchio (padre di Carolina, vittima di cyberbullismo) rivolto alle classi 4^a e 5^a sc. primaria e secondaria di Fontaneto.

2.2 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 e possiede generalmente una buona base di competenze e, nel caso delle figure di sistema, anche di carattere specialistico. Il percorso complesso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica e sulla sicurezza on-line può prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva all'interno dell'istituto e/o on-line, con la condivisione delle conoscenze dei singoli e il supporto dell'Animatore digitale, la partecipazione alle iniziative promosse dall'Amministrazione centrale e dalle scuole polo.

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

Nell'anno scolastico 2016/2017 (mese di Luglio), al fine di promuovere la condivisione di buone pratiche per un uso consapevole e sicuro delle ICT, e di prevenire e contrastare “ogni forma di

discriminazione e di bullismo, anche informatico” (Legge 107/2015, art. 1, c. 7, l), il nostro Istituto ha aderito al progetto “**Generazioni Connesse**” (SIC ITALY III), coordinato dal MIUR. Tale progetto prevede lo svolgimento di un Piano d’Azione che ha diversi ambiti di sviluppo, tra cui la formazione docente.

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

- organizzazione di Corsi di formazione per docenti e genitori;
- monitoraggio sul tema del cyberbullismo attraverso questionari;
- promozione della partecipazione di docenti, studenti e genitori a convegni e seminari sul tema del bullismo e del cyberbullismo;
- interventi di consulenza e supporto, relativamente a casi di bullismo e cyberbullismo.

2.4 Sensibilizzazione delle famiglie

La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento (*Policy e-safety*) per portare a conoscenza delle famiglie il regolamento sull’utilizzo delle nuove tecnologie all’interno dell’istituto e prevenire i rischi legati a un utilizzo non corretto di internet.

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

3.1 Accesso ad internet e Gestione accessi

L’istituto Ferrari è composto da:

- 3 plessi di scuola secondaria di secondo grado
- 5 Plessi di scuola primaria
- 5 Plessi di scuola dell’infanzia
- 1 Segreteria generale d’istituto

Tutti i plessi sono collegati alla rete internet; la maggioranza via ponte radio. L’accesso alla rete è di competenza del Comune dove sono ubicati i plessi. Quasi tutti gli apparati di comunicazione sono di proprietà degli stessi Comuni. Tutti i plessi hanno una rete WiFi interna.

Ci sono molte differenze negli aspetti dell’informatica dei diversi plessi, dovuti a vari fattori; ciò comporta che l’approccio alla E-policy debba essere necessariamente diverso.

Ogni plesso ha a disposizione un PC dedicato esclusivamente agli insegnanti, ed è l’unico che ha la possibilità di ricevere ed inviare posta con un client email.

Ogni aula di ogni plesso di scuola primaria e secondaria ha a disposizione un PC, laptop o fisso, connesso alla rete dell’istituto, utilizzato dagli insegnanti per la didattica. Non sono utilizzati dagli studenti.

- Le scuole dell'infanzia hanno dei PC portatili, che le maestre utilizzano nelle classi. Non sono utilizzati dai bambini.
- Le scuole primarie di Momo e Cressa hanno a disposizione un'aula informatica, ma praticamente inutilizzate.
- I plessi di scuola secondaria hanno a disposizione un'aula informatica che utilizzano regolarmente.

In pratica quindi solo gli alunni delle scuole secondarie hanno la possibilità di utilizzo, autonomo ma controllato, di PC con accesso alla rete.

La rete WiFi dei plessi è utilizzabile dai soli docenti e dai PC dei plessi, dimensionata per la didattica, e la password di accesso non è conosciuta dagli alunni, a cui quindi non è concesso l'utilizzo.

Le apparecchiature informatiche della segreteria dell'istituto hanno una regolamentazione riservata, la rete della segreteria non è accessibile al di fuori dall'edificio, e non è interessata dalle presenti policies.

Le regole di base relative all'accesso ad Internet faranno parte integrante del **Regolamento d'Istituto**, e saranno esposte all'albo dell'Istituto, all'interno dei laboratori di informatica.

Sarà cura del docente responsabile del laboratorio e dei vari docenti utenti del medesimo illustrare i contenuti delle norme per l'utilizzo delle TIC agli studenti, tenendo conto della loro età ed evidenziando le opportunità ed i rischi connessi all'uso della comunicazione tecnologica. I genitori saranno informati sulle E-policy d'istituto tramite la pubblicazione del regolamento sul sito web della scuola.

3.2 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. Le credenziali sono in possesso del personale amministrativo. La posta elettronica è protetta da antivirus e da antispam.

3.3 Sito web della scuola e servizi on-line a famiglie, studenti, docenti/utenti esterni.

L'accesso al sito web di istituto è libero, pertanto anche i materiali e i servizi disponibili per l'utenza (docenti, studenti e famiglie) sono liberamente fruibili e non viene richiesta alcuna password per la loro consultazione.

La scuola offre all'interno del proprio sito web i seguenti servizi alle famiglie ed agli utenti esterni: consultazione elenchi libri di testo; piano dell'offerta formativa; regolamento di istituto; informazioni generali sull'istituto; informazioni sui progetti attivati dall'istituto; informazioni sull'amministrazione dell'istituto; albo di istituto; avvisi e comunicazioni; moduli vari; circolari per i docenti; ed altro.

Sarà cura del responsabile della gestione delle pagine del sito della scuola vigilare che il contenuto sul sito sia appropriato. 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 non pubblicherà materiale prodotto dagli alunni senza il permesso dei loro genitori; inoltre, le fotografie degli stessi saranno pubblicate con il 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.

Nel sito web della scuola è presente anche un collegamento “esterno” al **registro elettronico**, strumento on-line facente le funzioni di registro di classe e registro personale del docente con accesso con credenziali da parte dei genitori per valutazioni, note, programmi svolti. Il servizio di Registro on-line non viene gestito dall’Istituto ma è fornito da una società esterna (Gruppo Spaggiari S.p.A). Tale piattaforma risiede su un altro server, pertanto essa risponde a criteri di *policy* non previsti dal presente documento.

L’Istituto si impegna a mantenere efficienti i servizi offerti, a migliorarli e estenderli nell’ottica di aumentare la qualità.

3.4 Social network.

A tutt’oggi, non si è reso necessario l’utilizzo dei social network nella didattica o, comunque, in ambito scolastico.

3.5 Protezione dei dati personali

Il trattamento dei dati personali riguarda unicamente le finalità istituzionali della scuola per le quali vengono raccolti solo i dati strettamente necessari. Essi saranno trattati con o senza l’ausilio di strumenti elettronici e comunque automatizzati secondo le modalità e le cautele previste dall’art. 13 del D.Lgs 196/2003 e conservati per il tempo necessario all’espletamento delle attività amministrative e istituzionali.

4. STRUMENTAZIONE PERSONALE

Studenti

Nell’Istituto non è consentito agli alunni di portare a scuola i telefoni cellulari. In caso di urgenza per comunicazioni tra gli alunni e le famiglie, su autorizzazione dei docenti e sotto il diretto controllo dei collaboratori scolastici, gli alunni potranno comunicare con le famiglie tramite gli apparecchi telefonici della scuola.

Per quanto concerne l'utilizzo dei tablet o PC portatili (Attività BYOD – *Bring your own device*), potranno essere utilizzati solo se permessi dal docente, alla presenza del docente e per ragioni prettamente scolastiche.

Docenti e altro personale

Durante le ore di lezione è consentito ai docenti l’uso di cellulari, PC portatili e tablet di loro proprietà unicamente a scopo didattico e ad integrazione dei dispositivi scolastici disponibili (Attività BYOD – *Bring your own device*).

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

5.1. Prevenzione

Rischi

Gli insegnanti, per la natura stessa del loro lavoro, devono in molti casi fungere da “torre di avvistamento”, avamposto privilegiato delle problematiche e dei rischi che bambini e adolescenti possono trovarsi ad affrontare ogni giorno.

Responsabilità degli insegnanti è, dunque, imparare a riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente. Tra questi, un’attenzione specifica andrà prestata ai fenomeni di:

- **bullismo/cyberbullismo** – una forma di prepotenza virtuale e non, attuata attraverso l’uso di internet e delle tecnologie digitali;
- **sexting** - pratica di inviare o postare messaggi di testo e immagini a sfondo sessuale, come foto di nudo o semi-nudo, via cellulare o tramite Internet;
- **adescamento o grooming** – una tecnica di manipolazione psicologica, che gli adulti potenziali abusanti utilizzano online, per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata;

I rischi che gli alunni possono correre a scuola derivano da un uso non corretto dei dispositivi elettronici, in particolare di quelli personali.

Azioni

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 il **Patto di Corresponsabilità** educativa previsto dallo Statuto delle studentesse e degli studenti della Scuola Secondaria. 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.

Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli studenti vi sono le seguenti:

- Diffondere un’informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web.
- Organizzare incontri con esperti (psicologo, Polizia Postale, ecc.) nelle singole classi e aventi per oggetto le tematiche del cyberbullismo, del sexting e dell’adescamento.
- Richiedere autorizzazione esplicita da parte dei genitori all’utilizzo dei dati personali degli alunni (es. liberatoria per la pubblicazione di foto, immagini, video relativi al proprio/a figlio/a per la partecipazione a progetti didattici e altro).
- Attento monitoraggio da parte del personale docente affinché il presente regolamento venga rispettato.
- Tempestivo intervento tramite opportuna sanzione qualora il regolamento venga disatteso.

5.2 Come segnalare: quali strumenti e a chi

Per il telefono cellulare ci si può assicurare che l'alunno vittima salvi nel suo telefono ogni messaggio, voce/testo/immagine, conservando così il numero del mittente.

Per le segnalazioni di fatti rilevanti si agirà conformemente a quanto stabilito nel Regolamento d'Istituto.

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

La presa in carico di situazioni di abuso sessuale, così delicate e complesse, richiede un approccio multidisciplinare, da parte di diverse figure professionali. L'intervento dovrebbe riguardare gli ambiti medico, socio-psicologico e giudiziario.

Il compito della scuola è quello di prevenire l'abuso e, nel caso questo avvenga, di aiutare l'eventuale vittima, in quanto ha al suo interno aspetti relazionali ed educativi che possono contribuire alla crescita serena del minore.

Per riuscire in questi intenti la scuola collabora con altre figure professionali e le famiglie, scambiando informazioni e condividendo progetti e prassi operative, favorendo occasioni di confronto e di dialogo.

Qualora siano coinvolti più alunni, in qualità di vittime o di responsabili della condotta scorretta, le famiglie degli alunni in questione saranno informate tempestivamente per un confronto.

In base all'entità dei fatti si provvederà a:

- Una comunicazione scritta tramite diario alle famiglie;
- Una nota disciplinare tramite registro elettronico;
- Una convocazione formale dei genitori degli alunni, tramite segreteria;
- Una convocazione delle famiglie da parte del Dirigente Scolastico.

Per i fatti più gravi la scuola si rivolgerà direttamente agli organi di polizia competenti.

La scuola non può intervenire su ciò che gli alunni svolgono fuori da essa con strumenti digitali ma qualora il docente venisse a conoscenza di eventuali atti scorretti come la condivisione di foto non autorizzate o l'insulto da parte di un alunno ad un compagno sul gruppo classe di WhatsApp (la creazione dei gruppi classe su WhatsApp è oggi una pratica molto diffusa) dovrà tempestivamente invitare le famiglie degli alunni coinvolti ad un attento monitoraggio delle attività svolte dai propri figli in rete.

5.3 Gestione dei casi.

Per quanto riguarda la gestione dei casi il nostro Istituto ha individuato una figura referente. La segnalazione del caso dovrà quindi essere fatta dal singolo docente, tramite modulo allegato al presente documento (*Allegato 1*), alla referente, la quale si occuperà di raccogliere tutte le informazioni possibili e di segnalare l'accaduto al Dirigente. Sarà poi il Dirigente a valutare se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali o se il caso vada gestito all'interno della scuola con il coinvolgimento del Consiglio di Classe e delle famiglie degli alunni coinvolti.

5.4 Definizione delle azioni da intraprendere a seconda della specificità del caso.

Casi di cyberbullismo

Si definiscono bullismo tutte quelle situazioni caratterizzate da volontarie e ripetute aggressioni mirate a insultare, minacciare, diffamare e/o ferire una persona (o a volte un piccolo gruppo). Si tratta, pertanto, di una serie di comportamenti portati avanti ripetutamente nel tempo. Si parla di cyberbullismo quando queste forme di prevaricazione reiterate nel tempo si estendono anche alla vita online.

Tale specifica forma di bullismo ha caratteristiche peculiari:

- È pervasivo: il bullo può raggiungere la sua vittima in qualsiasi momento e in qualunque luogo;
- È un fenomeno persistente: il materiale messo online vi può rimanere per molto tempo;
- Spettatori e cyberbulli sono potenzialmente infiniti: le persone che possono assistere agli atti di cyberbullismo sono potenzialmente illimitate;

Occorre tenere presente che il cyberbullo non è mai del tutto consapevole della gravità dei suoi comportamenti, se non viene aiutato ad esserne consapevole.

Qualora ci si trovi di fronte ad un caso di cyberbullismo (denunciato dalla vittima stessa, da persone vicino alla vittima o scoperto da un docente) si procederà nel modo seguente.

- Il docente venuto a conoscenza del fatto dovrà:
 - Informare tempestivamente la referente tramite modulo (*Allegato 1*);
 - Informare tempestivamente il Consiglio di Classe dell'alunno oggetto di cyberbullismo;
 - Informare i genitori dell'alunno oggetto di cyberbullismo, offrendo loro la possibilità di avere il supporto della psicologa della scuola per affrontare al meglio la situazione;
- La referente, in collaborazione con il CdC raccoglierà tutte le informazioni possibili;
- Il CdC:
 - valuterà, a seconda della gravità del caso, come sanzionare il/i responsabili (qualora sia stato possibile individuarli);
 - Con la collaborazione della psicologa della scuola, proporrà agli studenti attività durante le quali questi possano confrontarsi sull'accaduto;
- Il Dirigente valuterà se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali.

Casi di sexting

Con il termine sexting si intende l'invio e/o la ricezione e/o la condivisione di testi, video o immagini sessualmente esplicite tramite cellulare o tramite internet.

Qualora ci si trovi di fronte ad un caso di sexting (denunciato dalla vittima stessa, da persone vicino alla vittima o scoperto da un docente) si procederà in maniera analoga ai casi di cyberbullismo.

Casi di adescamento online o grooming

Le tecnologie digitali consentono ai giovani di ampliare la propria rete di amicizie in modo quasi smisurato: non di rado gli adolescenti "concedono" la loro amicizia non solo a persone che conoscono direttamente, ma anche ad "amici di amici". Questo li espone a rischi notevoli, come quello di dare accesso a sconosciuti al loro mondo online e quindi a informazioni personali. L'adescamento online (*grooming*) consiste nel tentativo, da parte di un adulto, di avvicinare un/a

bambino/a o adolescente per scopi sessuali, conquistandone la fiducia attraverso l'utilizzo della rete Internet (tramite chat, blog, forum e social networks, per esempio). In un primo tempo, l'adulto, spesso mentendo sulla propria identità e sulla propria età, mostra particolare interesse nei confronti del/la bambino/a o dell'adolescente, cercando di conquistarne la fiducia. Solo in un secondo tempo, cerca di entrare sempre più nell'intimità del bambino fino a introdurre argomenti intimi e attinenti alla sfera sessuale.

È bene che anche gli insegnanti aiutino i propri alunni a tutelarsi, scegliendo con cura chi frequentare online, per evitare che una condotta imprudente possa comportare ripercussioni non banali nella loro vita reale.

Una volta riconosciuti alcuni segni che possono rinviare a una situazione di adescamento online, quali un improvviso calo nel rendimento scolastico; un aumento del tempo trascorso dall'alunno online congiunto ad una particolare riservatezza al riguardo, allusioni da parte dell'alunno alla frequentazione di una persona più grande, o a regali ricevuti, ecc., si procederà nel modo seguente.

- Il docente venuto a conoscenza del fatto dovrà:
 - Informare tempestivamente la referente tramite modulo;
 - Informare tempestivamente il Consiglio di Classe dell'alunno oggetto di adescamento;
 - Informare i genitori dell'alunno oggetto di adescamento, offrendo loro la possibilità di avere il supporto della psicologa della scuola per affrontare al meglio la situazione.
- La referente in collaborazione con il CdC raccoglierà tutte le informazioni possibili;
- Il CdC con la collaborazione della psicologa della scuola, proporrà agli studenti attività durante le quali gli alunni possano confrontarsi con la tematica in oggetto;
- Il Dirigente valuterà se la segnalazione debba essere rivolta ad organi esterni alla scuola quali la Polizia Postale o i Servizi Sociali.

F.to Il Dirigente
Prof. Gerardo Pedullà



F.to La Referente
prof. M. Federica Pellegrino



ALLEGATO 1

MODULO PER LA SEGNALAZIONE

(Il presente modulo va compilato dal docente che raccoglie la segnalazione con la collaborazione dello studente)

- Episodio di:
 - Bullismo
 - Cyberbullismo
 - Sexting
 - Grooming
- Alunni coinvolti:
 - Vittima/e _____
 - Responsabile/i _____
- Quando? _____
- Dove? _____
- Descrizione del fatto _____

Data _____

Il docente

ALLEGATO 2



Sicurezza in rete - Schema per la scuola



Schema riepilogativo delle situazioni gestite legate a rischi online (ALLEGATO N.2)

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?		