UNIONE EUROPEA
FONDI STRUTTURALI EUROPEI
PON 2014-2020
PER LA SCUOLA - COMPETENZE E AMBIENTI PER L'APPRENDIMENTO-FESR
Ministero dell'Istruzione, dell'Università e della Ricerca
Dipartimento per la Programmazione
Direzione Generale per interventi in materia di edilizia scolastica, per la gestione dei fondi strutturali per l'istruzione e per l'innovazione digitale
Ufficio IV
MIUR

Ministero dell'Istruzione dell'Università e Ricerca

ISTITUTO COMPRENSIVO "A. MANZONI" MESOLA
Via Gramsci n. 38 – 44026 MESOLA – (Ferrara) C.F. 91010690385
C.M. FEIC801009 - Codice Univoco Ufficio UF2C8F – Codice IPA istsc_feic801009
☎ 0533.993718 – 993249 🖷 0533.993718 - Presidenza 0533.993343
www.icmesola.gov.it
e-mail: feic801009@istruzione.it
p.e.c.: FEIC801009@PEC.ISTRUZIONE.IT

Generazioni Connesse
SAFER INTERNET CENTRE

Policy di E-Safety

1. Introduzione

La presenza sempre più diffusa delle tecnologie digitali nella vita di tutti i giorni apre nuove opportunità ma pone nuove attenzioni dal punto di vista dell'utilizzo sicuro, consapevole e positivo.
Lo sviluppo e l'integrazione dell'uso delle Tecnologie dell'Informazione e della Comunicazione (TIC), ed in particolare di Internet, nella didattica offrono le condizioni e l'occasione per una trasformazione concreta della relazione insegnamento/apprendimento
Per questo l'IC "A. Manzoni" ha deciso di munirsi di un documento di policy di e-safety per formare i propri docenti ed i propri studenti ad un uso corretto e responsabile delle TIC e porre l'opportuna attenzione alla sicurezza digitale affinché i nuovi strumenti digitali vengano utilizzati in modo positivo e responsabile.

1.1 Scopo della Policy.

Lo scopo di questo documento è:
- Stabilire norme comportamentali e procedure per facilitare e promuovere l'utilizzo delle TIC;
- Stabilire misure di prevenzione, rilevazione e gestione delle problematiche connesse a un uso non consapevole delle tecnologie digitali;
- Stabilire procedure chiare per affrontare un uso improprio degli strumenti digitali o gli abusi online come il cyber bullismo;
- Informare tutti i membri della comunità scolastica per renderli consapevoli del fatto che i comportamenti illeciti o pericolosi sono inaccettabili e che

verranno intraprese azioni appropriate, disciplinari e/o giudiziarie quando la situazione lo richiederà.

1.2 Ruoli e Responsabilità

Dirigente Scolastico

- è garante della sicurezza online dei membri della comunità scolastica;

- offre a tutti gli insegnanti una formazione adeguata in merito a un utilizzo positivo e responsabile delle TIC;

- segue 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;

Direttore dei Servizi Generali e Amministrativi:

- registra disservizi e problematiche relative alla rete e all'uso del digitale comunicate dalla persona incaricata dal Dirigente;

- assicura, nei limiti delle risorse finanziarie disponibili, interventi di manutenzione richiesti per cattivo funzionamento e/o danneggiamento della dotazione tecnologica dell'Istituto;

- facilita trasmissione di comunicazioni relative alle tecnologie digitali tra le varie componenti della scuola;

Animatore digitale

- promuove l'aggiornamento dei docenti;

- propone e promuove l'uso delle TIC;

- monitora e rileva problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola;

- propone la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili;

- assicura che gli utenti possano accedere alla rete della scuola solo tramite password;

Responsabile/i della gestione delle apparecchiature e della rete (Team digitale):

- registra disservizi e problematiche relative alla rete e all'uso del digitale e le comunica al DSGA

- tiene il registro delle problematiche e dei controlli periodici di manutenzione hardware e della rete;

- richiede interventi ordinari e straordinari per eventuali malfunzionamenti (pronto soccorso digitale).

Docente/i:

- applica le norme fissate dalla POLICY (sorveglianza alunni e norme utilizzo TIC)

- garantisce che l'alunno capisca e segua le regole della policy per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;

- comunica ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;

- segnala 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;

- segnala 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.

- propone eventi di prevenzione e sensibilizzazione in merito al Cyberbullismo, all'educazione all'affettività ecc, anche chiedendo la collaborazione di Agenzie-Istituzioni del Territorio

Alunni:

- Utilizzano le TIC

- Rispettano le norme fissate dalla POLICY

Genitori degli alunni

- Partecipano agli eventi promossi e organizzati dalla scuola

- Condividono le norme contenute nella POLICY di e Safety

Ata

- Conoscono le norme della policy

- Contribuiscono alla sorveglianza

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

1.3.1 Condivisione e comunicazione Personale

- Le regole adottate dalla scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet saranno proposte e discusse negli organi collegiali (collegio docenti, riunioni di dipartimento, consigli di classe) e rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito web della scuola;
- Al personale della scuola sarà offerta la possibilità di seguire un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso materiali resi disponibili anche sul sito web della scuola e corsi tenuti da esperti interni o esterni.

1.3.2 Condivisione e comunicazione Genitori

- Le famiglie saranno informate in merito alla linea di condotta adottata dalla scuola per un uso sicuro e responsabile delle tecnologie digitali e di internet attraverso la condivisione del presente documento e di materiali informativi specifici sul sito web della scuola;
- Al fine di sensibilizzare le famiglie sui temi dell'uso delle TIC ed ai pericoli ad esse connessi saranno organizzati dalla scuola incontri informativi.

1.3.3 Condivisione e comunicazione Alunni

- All'inizio dell'anno, in occasione dell'illustrazione del regolamento d'istituto agli alunni da parte dei docenti, verrà presentata questa policy, insieme ai regolamenti correlati;
- Nel corso dell'anno saranno proposte alcune lezioni sulle buone pratiche per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta al cyberbullismo.

1.4 Gestione delle infrazioni alla Policy.

In relazione a quanto specificato in questa policy, ed in particolare ai ruoli dei vari soggetti coinvolti, le infrazioni saranno gestite in modo graduale rispetto alla gravità e, nel caso degli alunni, anche alla loro età.

1.4.1 Infrazioni degli alunni.

I docenti possono introdurre, preventivamente, attività laboratoriali mirate a sviluppare negli alunni una sempre maggiore consapevolezza dei rischi legati ad un uso imprudente e improprio del web in modo da fornire loro, ogniqualvolta avvenga un'infrazione alle regole stabilite, gli strumenti per affrontare le conseguenze dei loro errori.

Le potenziali infrazioni a carico degli alunni sono identificabili in:

- uso di social network e blog per pubblicare, condividere o, in genere, postare commenti o giudizi offensivi che ledano la privacy altrui;
- condivisione di dati personali che possano permettere l'identificazione;
- connessioni a siti proibiti o comunque non autorizzati;
- pubblicazione di foto o immagini non autorizzate e/o compromettenti.

I provvedimenti disciplinari da adottare da parte del consiglio di classe nei confronti dell'alunno che ha commesso un'infrazione alla policy saranno i seguenti:

- richiamo verbale;
- sanzioni estemporanee commisurate alla gravità della violazione commessa (assegnazione di attività aggiuntive da svolgere a casa su temi di Cittadinanza e Costituzione, …);
- nota informativa sul diario ai genitori;
- nota disciplinare sul registro ;
- convocazione dei genitori per un colloquio con l'insegnante;
- convocazione dei genitori per un colloquio con il Dirigente scolastico.

1.4.2 Infrazioni del personale scolastico.

Le infrazioni alla policy da parte del personale scolastico possono essere delle seguenti tipologie:

- mancata osservanza delle regole qui descritte sulla gestione della strumentazione, in tal caso la gravità dell'infrazione sarà valutata in funzione del rischio a cui sono stati esposti gli alunni;
- Fatta salva l'imprevedibilità della violazione, la mancata sorveglianza e pronto intervento nel caso di infrazione da parte degli alunni , sarà valutata in funzione del danno per la non tempestiva attivazione delle azioni indicate nel presente documento.

1.4.3 Infrazioni dei genitori.

Compito preciso dei genitori è supportare gli insegnanti e il personale scolastico nel riconoscimento e nella costruzione di azioni di contrasto efficaci ai principali rischi rappresentati dalla navigazione internet di utenti molto giovani e spesso poco accorti. Nel caso di infrazione si prevedono interventi, rapportati alla gravità, che vanno dalla semplice comunicazione del problema alla convocazione da parte dell'insegnante di classe o del Dirigente Scolastico.

1.5 Monitoraggio dell'implementazione della Policy e suo aggiornamento.

Il monitoraggio dell'implementazione della policy e del suo eventuale aggiornamento sarà curato dal Dirigente scolastico con la collaborazione del Team digitale. Tale monitoraggio 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 ai docenti, al fine di valutare l'impatto della policy e la necessità di eventuali miglioramenti. L'aggiornamento della policy sarà curato dal Dirigente scolastico, dal Team digitale.

1.6 Integrazione della Policy con Regolamenti esistenti.

Il presente documento sarà allegato al Regolamento di Istituto e inserito nel sito web della scuola.
I genitori saranno informati della pubblicazione della policy di e-safety della scuola e possono prenderne visione sul sito della scuola e partecipare ad attività di informazione/formazione.

2. Formazione e Curricolo

2.1 Curricolo sulle competenze digitali per gli studenti.

Le competenze digitali sono definite dalle "Raccomandazioni del parlamento europeo in relazione alle competenze chiave per l'apprendimento permanente come segue: "*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.[…] L'uso delle TSI comporta un'attitudine critica e riflessiva nei confronti delle informazioni disponibili e un uso responsabile dei mezzi di comunicazione interattivi. Anche un interesse a impegnarsi in comunità e reti a fini culturali, sociali e/o professionali serve a rafforzare tale competenza."

Il traguardo di competenza che viene estrapolato per il nostro Istituto è il seguente: lo studente utilizza in sicurezza e con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo.

Il livello raggiunto è identificato dagli indicatori:

A. Avanzato: L'alunno/a svolge compiti e risolve problemi complessi, mostrando padronanza nell'utilizzo delle conoscenze e delle abilità associate ad internet ed alle tecnologie digitali; propone e sostiene le proprie opinioni e assume in modo responsabile decisioni consapevoli.

B. Intermedio: L'alunno/a svolge compiti e risolve problemi in situazioni nuove, compie scelte consapevoli , mostrando di saper utilizzare le conoscenze e le abilità associate ad internet ed alle tecnologie digitali.

C. Base: L'alunno/a svolge compiti semplici anche in situazioni nuove, mostrando di possedere conoscenze e abilità fondamentali e di saper applicare regole basilari e procedure apprese per un utilizzo sicuro di internet e delle TIC.

D. Iniziale: L'alunno/a, se opportunamente guidato/a, svolge compiti semplici in situazioni note.

2.2 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 si propongono i seguenti ambiti di formazione:

- Proposte di corsi di formazione mirati all'utilizzo concreto (esperienze in aula) delle TIC nella didattica ed in particolare:
    - Proposte di formazione sull'uso di piattaforme digitali per la didattica
    - Proposte di formazione all'utilizzo del Registro elettronico;
    - Proposte di formazione sul Coding
    - Proposte di formazione su suite di condivisione (es. G-apps)
- Ciascun corso di formazione potrebbe concludersi con la stesura e la messa a disposizione, sul sito istituzionale della scuola, di Manuali, Guide e Tutorial per l'utilizzo specifico delle diverse TIC;
- Condivisione delle conoscenze dei singoli unito al supporto dell'Animatore digitale e del Team per l'innovazione previsto dal PNSD.

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

La formazione dei docenti sull'utilizzo consapevole e sicuro di internet e delle tecnologie digitali potrà prevedere momenti di autoaggiornamento, momenti di

formazione personale in presenza o a distanza e momenti di formazione 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.

Nello specifico la formazione proposta dall'istituto prevede:

- Organizzazione di corsi interni, per favorire uno sviluppo professionale proattivo; con particolare attenzione alla promozione di approcci e culture nuove nei confronti del proprio ruolo e dei compiti ad esso connessi;
- favorire la partecipazione a corsi esterni inerenti la didattica innovativa per ogni singola disciplina e/o che rispondano ad esigenze formative del sistema scolastico nel suo complesso.

Per proporre tale formazione si ricorrerà alle risorse sotto indicate:

- personale docente interno alla scuola che abbia acquisito competenze in determinati settori affini alle esigenze sopra evidenziate;
- soggetti esterni che offrano la possibilità di mettere in opera un'attività di consulenza mediante seminari e incontri-dibattito;
- formazione a distanza (e-learning).

2.4 Sensibilizzazione delle famiglie.

Per favorire la sinergia degli interventi educativi di scuola e famiglia per il successo scolastico ed educativo di ogni studente, il presente documento, assieme al Patto Educativo di Corresponsabilità stipulato con le famiglie degli alunni è a disposizione sul sito web d'Istituto.

Verranno inoltre valorizzate le opportunità di incontro e informazione per le famiglie sui temi oggetto della Policy, offerte dal territorio, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità:

- Incontri con la Guardia di Finanza;
- Incontri con la Polizia Postale;
- Altri enti e/o associazioni.

I genitori saranno tenuti aggiornati sulle attività svolte dagli studenti in campo digitale in modo da coinvolgerli attivamente.

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

3.1 Accesso ad internet

Tutti i plessi dell'Istituto possiedono una rete di accesso internet LAN E WLAN. In ogni aula didattica è possibile accedere alla linea ethernet per usufruire dei pc a supporto delle LIM.

Negli uffici di segreteria le postazioni sono fisse e accedono alla rete con un canale separato rispetto ai pc delle aule didattiche e agli spazi comuni dei docenti.

Nell'Istituto comprensivo sono presenti 3 aule informatica dislocate su 3 plessi di scuola Primaria e Secondaria di primo grado, tutte con accesso LAN e WLAN.

La rete LAN nelle aule informatica è protetta da DNS con parental control. I pc sono numerati per poter organizzare e gestire con maggior precisione l'attività degli alunni.

I computer dell'Istituto possiedono antivirus integrati e di terze parti nelle postazioni della segreteria i quali vengono aggiornati per le licenze dal responsabile degli strumenti informatici nominato dal Dirigente scolastico.

3.2 Gestione degli accessi

L'istituto possiede una rete wireless con più livelli di accesso:

-rete docenti

-rete ospiti

-rete IC Manzoni

Per accedere al WI-FI è necessario accreditarsi con nome utente e password assegnati dall'ufficio di segreteria. La gestione (cancellazione e creazione) delle password è a cura del Gestore della rete dati.

I computer presenti nelle aule che permettono l'utilizzo delle LIM, richiedono l'inserimento dell'ID che i docenti avranno cura di non diffondere tra gli studenti.

I computer presenti nelle aule informatica devo essere configurati con account amministratore protetto da password.

Il personale ATA degli uffici accede alla rete WLAN con le stesse modalità dei docenti.

3.3 **E-Mail**

La segreteria, il Dirigente e i suoi collaboratori comunicano con i docenti e le famiglie attraverso il registro elettronico.

Ogni ordine di scuola inoltre, utilizza un account Google per la posta elettronica: i docenti usufruiscono dell'account esclusivamente per scopi professionali. È a cura del docente referente di plesso la manutenzione del suddetto account.

3.4 Sito web

L'istituto possiede uno spazio web con dominio www.icmesola.gov.it. La gestione del sito avviene attraverso il pannello di controllo amministratore da parte del docente con funzione strumentale.

Le informazioni pubblicate sul sito relative ai contatti delle persone rispettano le norme vigenti sulla privacy. I contenuti, le informazioni e le immagini sono pubblicate con riguardo particolare alla tutela della privacy dei minori e del personale scolastico.

L'area "*amministrazione trasparente*" e "*albo online*" sono gestite dal personale amministrativo attraverso la segreteria digitale.

3.5 Social network

Ogni docente può, all'interno della propria programmazione didattica, utilizzare varie piattaforme e-learning a scopo didattico con gli alunni e a scopo professionale, con altri docenti. Tali piattaforme consentono una comunicazione docente-studente protetta.

Qualsiasi docente che ritenga necessario utilizzare i canali social per interagire con gli studenti a livello didattico (comunicazione docente-studente non protetta), si assume la completa responsabilità.

3.6 Protezione dei dati personali

L'Istituto protegge i dati personali nel rispetto della privacy dei propri utenti. Al momento della raccolta di dati personali, vengono illustrate le modalità di trattamento dei dati all'utente e le finalità di raccolta. L'Istituto non comunicherà i dati personali dell'utente a terzi senza il consenso dello stesso. La scuola potrà comunicare i dati raccolti all'interno dell'Istituto od a terzi che prestano servizi alla scuola, solo con il permesso dell'utente. La scuola tratta i dati personali dell'utente per soddisfare le richieste a specifici servizi (es: registro elettronico), per aggiornare l'utente sulle ultime novità in relazione ai servizi offerti od altre informazioni che ritiene siano di interesse dell'utente che provengono direttamente dall'Istituto o dai suoi partners, e per comprendere meglio i bisogni dell'utente ed offrire allo stesso servizi migliori (vedi Allegato consenso ex art.23).

4. Strumentazione personale

Non è permesso agli studenti utilizzare i propri dispositivi durante le attività didattiche così come previsto dal regolamento disciplinare. Gli studenti non possono accedere alla rete della scuola se non autorizzati dagli insegnanti ed esclusivamente per scopi attinenti le attività didattiche.

I docenti possono utilizzare i propri dispositivi ed usufruire dell'accesso alla rete esclusivamente per uso professionale.

5. Prevenzione, gestione e rilevazione dei casi

Prevenzione

RISCHI

L'utilizzo eccessivo o errato delle tecnologie o di internet da parte di minori, che riguardi la navigazione incontrollata nella rete, l'interazione tramite social network, giochi on-line o lo scambio di sms, può portare a conseguenze altamente negative se avviene senza la supervisione dell'adulto e soprattutto in modo prolungato, sia dal punto di vista psicologico che relazionale:

Risvolti psicologici ed emotivi

- Isolamento
- Depressione
- Dipendenza
- Disorientamento e difficoltà di distinzione tra il reale e il virtuale
- Sviluppo di sintomi compulsivi
- Rischio di ripercussioni anche a livello scolastico
- Rischio di ripercussioni nei rapporti con la famiglia
- Errata percezione della propria identità
- Senso di onnipotenza
- Tendenza alla violenza

Risvolti relazionali e sociali

- Paura dell'esclusione dal gruppo (ansia e attacchi di panico)
- Sviluppo di meccanismi disfunzionali:
  - Depersonalizzazione
  - Senso di onnipotenza
  - Tendenza alla violenza
- Conseguente predisposizione a divenire vittima di cyber bullismo o a commettere atti di cyber bullismo
- Alta probabilità di venire a contatto con truffe, pedopornografia, adescamento, furto d'identità

AZIONI

Le azioni che la scuola può predisporre ed applicare per prevenire comportamenti sconvenienti da parte di minori, o scongiurare i rischi sopraccitati, saranno le seguenti:

- **Sicurezza informatica**: l'istituto farà attenzione a disciplinare scrupolosamente gli accessi al web, è inoltre richiesto il rigoroso rispetto del regolamento relativamente al divieto di uso dei cellulari.

- **Formazione docenti**: si provvederà ad una formazione specifica rivolta ai docenti per quanto riguarda l'utilizzo consapevole e sicuro delle tecnologie digitali.

- **Interventi educativi**: un ulteriore tipo di prevenzione è costituito dagli interventi di tipo educativo, inseriti nella Politica Scolastica, compresa quella anti-cyberbullismo, definita e promossa dal Dirigente e da mettere in atto in collaborazione con tutte le componenti della scuola e con i genitori.

- La somministrazione di **questionari** anonimi agli studenti delle classi quinte della Scuola Primaria e delle classi prime e seconde della Scuola Secondaria di 1^ Grado, in modo da poter individuare eventuali casi e situazioni di cyber bullismo, da predisporre per il mese di aprile di ogni anno scolastico. Se possibile, si può predisporre una compilazione su piattaforma online. Altrettanto importante è la restituzione dei dati e la condivisione con gli alunni in spazi e momenti dedicati allo scopo.

- La discussione aperta e **l'educazione trasversale all'inclusione,** la creazione di un ambiente che favorisca la relazione tra pari.

- La **promozione di progetti** dedicati all'argomento, con l'eventuale contributo esterno di figure professionali come psicologi, in cui si insegni agli alunni come tutelarsi, creando in loro la consapevolezza dei rischi che si corrono in rete.

- La messa a disposizione di una **casella mail** a cui gli studenti si possono riferire o alla quale possono denunciare eventuali episodi, o eventualmente la predisposizione di apposite postazioni in cui posizionare cassette di posta, ove gli alunni possano inserire comunicazioni o richieste d'aiuto scritte manualmente..

- **La collaborazione con l'esterno:** può avvenire tramite azioni di supporto, di monitoraggio e di dialogo costante con **enti locali, polizia locale, ASL di zona, Tribunale dei Minori, associazioni del territorio e/o nazionali** e incontri a scuola con le **Forze dell'Ordine**, nell'ambito di progetti tesi ad attivare la riflessione sul rispetto delle persone e delle cose, sulle conseguenze del proprio comportamento e sulla responsabilità di contribuire a costruire un ambiente accogliente e sereno per tutti, diffondendo la cultura del rispetto e della non violenza fra le giovani generazioni;

- **Incontri con le famiglie** per informare, dare indicazioni sulle possibilità di intervento e favorire la collaborazione con la scuola.
  Le famiglie, informate anche delle loro responsabilità e delle conseguenze legali dei comportamenti dei figli, dovranno essere attente a fare un'adeguata vigilanza, cercando di controllare e monitorare le amicizie virtuali e i siti frequentati dai figli e condividendo con loro le motivazioni di tale controllo.

Rilevazione

CHE COSA SEGNALARE

- Infrazione da parte di uno o più alunni delle regole, previste dal Regolamento Scolastico, inerenti l'utilizzo dei cellulari in ambiente scolastico o delle tecnologie informatiche in dotazione alla scuola senza la supervisione dei docenti.
- Cambiamenti radicali nel comportamento di un alunno, che possa essere stato vittima di azioni riconducibili al cyber bullismo: isolamento, evitamento nelle relazioni, attacchi d'ansia, calo nel rendimento scolastico.
- Atteggiamenti di scherno o intimidazione nei confronti di compagni.

COME SEGNALARE

- Per quanto concerne il personale della scuola, sarà compito di ogni docente o operatore riferire le proprie osservazioni e informazioni ai referenti o direttamente al Dirigente Scolastico.
- Nel caso in cui fosse un alunno ad essere vittima o testimone di comportamenti contrari alle regole o di cyber bullismo, sarà loro possibile effettuare una segnalazione attraverso i seguenti canali:
  Lettera anonima;
  Questionario;
  Helpline quali STOP e TELEFONO AZZURRO, presenti anche nella piattaforma di Generazioni Connesse.

  Sarà ovviamente cura dei docenti promuovere le suddette forme di segnalazione presso le classi durante i momenti formativi relativi all'argomento che saranno organizzati durante l'anno.

COME GESTIRE LE SEGNALAZIONI

Per quanto concerne le lettere inviate dagli alunni e la compilazione dei questionari anonimi, di particolare importanza sarà una celere elaborazione, per attuare in tempi brevi eventuali interventi.
Altrettanto importante è la restituzione dei dati e la condivisione con gli alunni in spazi e momenti dedicati allo scopo.

Gestione dei dati

DEFINIZIONE DELLE AZIONI DA INTRAPRENDERE PER LA GESTIONE CONDIVISA DEI DATI
I dati rilevati saranno condivisi dal team docente interessato dal caso emerso, alla presenza del Dirigente Scolastico.
Nei casi che richiederanno provvedimenti sanzionatori, saranno previsti Consigli di Classe Straordinari per discutere del caso anche in presenza della famiglia.
Per quanto riguarda le misure correttive e i parametri da adottare, si fa riferimento al Regolamento d'Istituto già in vigore.

Mesola 26 Aprile 2018

La Dirigente scolastica
Dott.ssa Antonietta Allegretta
(Firma autografa sostituita a mezzo stampa ai sensi
art. 3 comma 2) del D.Lgs. 39/1993)

Il gruppo di lavoro e-safety
(Micaela Cori, Barbara Duò,
Giulia Mantovani, Damiano Seghi)

Allegati
Linee guida per il docente
Linee guida per lo studente
Linee guida per i genitori
Questionario anonimo studente
Scheda di monitoraggio annuale

Ministero dell'Istruzione dell'Università e Ricerca	ISTITUTO COMPRENSIVO "A. MANZONI" MESOLA
	Via Gramsci n. 38 – 44026 MESOLA – (Ferrara) C.F. 91010690385
	C.M. FEIC801009 - Codice Univoco Ufficio UF2C8F – Codice IPA istsc_feic801009
	☎ 0533.993718 – 993249 🖷 0533.993718 - Presidenza 0533.993343
	www.icmesola.gov.it — e-mail: feic801009@istruzione.it — p.e.c.: FEIC801009@PEC.ISTRUZIONE.IT

PROTOCOLLO CYBERBULLISMO

LINEE GUIDA PER DOCENTI

Sicurezza della rete senza fili (Wireless – Wi-Fi)

L’Istituto dispone di una rete con tecnologia WLAN.

La rete wireless offre copertura in tutti i locali della scuola.

L’accesso alla rete wireless è regolato da AP che determinano l’accesso degli utenti dietro richiesta di credenziali (nome utente e password).

AZIONI:

• evitate di lasciare le email o file personali sui computer o sul server della scuola;

• salvate sempre i vostri lavori (file) in cartelle personali e/o di classe sui dispositivi di memorizzazione di rete (NAS) e non sul desktop o in altre posizioni in locale.

• discutete con gli alunni del Protocollo “Sicurezza in rete” della scuola e degli eventuali problemi che possono verificarsi nell’uso di Internet;

• date chiare indicazioni su come si utilizza Internet, ed eventualmente anche la posta elettronica, e informateli che le navigazioni saranno monitorate;

• ricordate di verificare lo stato dei computer alla fine della sessione di lavoro;

• ricordate agli alunni che la violazione consapevole del Protocollo “Sicurezza in rete” della scuola comporta la temporanea sospensione dell’accesso ad Internet per un periodo commisurato alla gravità del fatto. La violazione o il dolo accertati, oltre all’intervento disciplinare del consiglio di classe o team docente, daranno luogo alla richiesta di risarcimento delle ore perse per ripristinare il sistema e renderlo nuovamente operante ed affidabile; rimangono comunque applicabili ulteriori sanzioni disciplinari, azioni civili per danni, nonché l’eventuale denuncia del reato all’autorità giudiziaria. Nel caso di infrazione consapevole da parte dei docenti sarà compito del Dirigente Scolastico intervenire per via amministrativa secondo le norme vigenti e il regolamento di Istituto.

Consigli:

• Il bullismo è una dinamica relazionale di gruppo. Considerate che i ragazzi tendenti all'isolamento sono più a rischio di cadere vittima di atti di bullismo.

• L'atto di bullismo non si esemplifica in una singola condotta di prepotenza, ma si costruisce nel tempo confermando i ruoli di vittima, bullo e spettatore. Quindi in un progetto educativo, di controllo e prevenzione del fenomeno, occorre coinvolgere tutti i protagonisti (vittima, bullo e spettatore) e i genitori.

• Organizzate dei gruppi di discussione e confronto sul fenomeno prendendo spunto anche dalle notizie di cronaca.

• Coinvolgete attivamente i genitori e concordate un’alleanza educativa di confronto e prevenzione.

• Tenete in considerazione che ogni azione educativa deve essere rivolta a tutto il gruppo classe e non deve limitarsi al biasimo del singolo bullo.

• Soprattutto se avete una classe al primo anno di un ciclo di studi, investite un po' del vostro tempo a curare le relazioni dei ragazzi in classe per trasformare un insieme casuale di studenti in un gruppo sereno e armonioso.

• Curate i momenti di incontro extrascolastici come gite, visite ai musei, ai teatri, etc. per favorire l'integrazione del gruppo.

• Considerate che i momenti in cui la maggior parte dei bulli agisce indisturbata sono le pause dedicate alla ricreazione e alla mensa.

• Tenete presente che per facilitare il racconto di ciò che sta accadendo potrebbe essere utile l'istituzione di una linea telefonica, per genitori e vittime, a cui rivolgersi.

• Prendete in considerazione che potrebbe essere utile anche adottare una "cassetta postale delle prepotenze" dove lasciare dei biglietti in cui si racconta ciò che succede, in forma anonima all'inizio.

• Abituate i ragazzi a raccontare ciò che accade e a non nascondere la verità.

N.B.: i docenti dovranno raccogliere segnalazioni ed episodi di bullismo e/o cyberbullismo, compilare apposito modulo e consegnarlo in segreteria, debitamente firmato.

UNIONE EUROPEA
FONDI STRUTTURALI EUROPEI
PON 2014-2020
PER LA SCUOLA - COMPETENZE E AMBIENTI PER L'APPRENDIMENTO-FESR
Ministero dell'Istruzione, dell'Università e della Ricerca
Dipartimento per la Programmazione
Direzione Generale per interventi in materia di edilizia scolastica, per la gestione dei fondi strutturali per l'istruzione e per l'innovazione digitale
Ufficio IV
MIUR

Ministero dell'Istruzione dell'Università e Ricerca

ISTITUTO COMPRENSIVO "A. MANZONI" MESOLA
Via Gramsci n. 38 – 44026 MESOLA – (Ferrara) C.F. 91010690385
C.M. FEIC801009 - Codice Univoco Ufficio UF2C8F – Codice IPA istsc_feic801009
☎ 0533.993718 – 993249 🖷 0533.993718 - Presidenza 0533.993343
www.icmesola.gov.it
e-mail: feic801009@istruzione.it
p.e.c.: FEIC801009@PEC.ISTRUZIONE.IT

PROTOCOLLO CYBERBULLISMO

LINEE GUIDA PER STUDENTI

Sicurezza della rete senza fili (Wireless – WiFi)

L’Istituto dispone di una rete con tecnologia WLAN.

La rete wireless offre copertura in tutti i locali della scuola.

L’accesso alla rete wireless è regolato da AP che determinano l’accesso degli utenti dietro richiesta di credenziali (nome utente e password) . L’ottenimento delle credenziali è riservato al personale dell’Istituto, previa richiesta dietro compilazione di apposito modulo, da richiedere all’Amministratore di Rete.

Le regole di comportamento sono analoghe a quelle per la connessione alle reti cablate di Istituto.

Studenti

• Non utilizzate giochi né in locale, né in rete;

• salvate sempre i vostri lavori (file) in cartelle personali e/o di classe sui dispositivi di memorizzazione di rete (NAS) e non sul desktop o in altre posizioni in locale;

• mantenete segreto il nome, l’indirizzo, il telefono di casa, il nome e l’indirizzo della vostra scuola;

• non inviate a nessuno fotografie vostre o di vostri amici;

• chiedete sempre al vostro insegnante o ad un adulto il permesso di scaricare documenti da Internet;

• chiedete sempre il permesso prima di iscrivervi a qualche concorso o prima di riferire l’indirizzo della vostra scuola;

• riferite al vostro insegnante se qualcuno vi invia immagini che vi infastidiscono e non rispondete; riferite anche al vostro insegnante se vi capita di trovare immagini di questo tipo su Internet;

• se qualcuno su Internet vi chiede un incontro di persona, riferirlo al vostro insegnante, comunque ad un adulto;

• ricordatevi che le persone che incontrate nella rete sono degli estranei e non sempre sono quello che dicono di essere;

• non è consigliabile inviare mail personali, perciò rivolgetevi sempre al vostro insegnante prima di inviare messaggi di classe;

• non caricate o copiate materiale da Internet senza il permesso del vostro insegnante o del responsabile di laboratorio.

Ministero dell'Istruzione dell'Università e Ricerca

ISTITUTO COMPRENSIVO "A. MANZONI" MESOLA
Via Gramsci n. 38 – 44026 MESOLA – (Ferrara) C.F. 91010690385
C.M. FEIC801009 - Codice Univoco Ufficio UF2C8F – Codice IPA istsc_feic801009
☎ 0533.993718 – 993249 🖷 0533.993718 - Presidenza 0533.993343
www.icmesola.gov.it
e-mail: feic801009@istruzione.it
p.e.c.: FEIC801009@PEC.ISTRUZIONE.IT

PROTOCOLLO CYBERBULLISMO

LINEE GUIDA PER GENITORI

Sicurezza della rete senza fili (Wireless – WiFi)

L'Istituto dispone di una rete con tecnologia WLAN.

La rete wireless offre copertura in tutti i locali della scuola.

L'accesso alla rete wireless è regolato da AP che determinano l'accesso degli utenti dietro richiesta di credenziali (nome utente e password). L'ottenimento delle credenziali è riservato al personale dell'Istituto, previa richiesta dietro compilazione di apposito modulo, da richiedere all'Amministratore di Rete.

Le regole di comportamento sono analoghe a quelle per la connessione alle reti cablate di Istituto.

Segnali ai quali i genitori dovrebbero fare attenzione

• si rifiuta di parlare di ciò che fa online;

• utilizza Internet fino a tarda notte;

• fa un uso eccessivo di Internet;

• ha un calo dei voti scolastici;

• è turbato dopo aver utilizzato Internet.

Interventi per i genitori:

FARE:

• tenere il computer in una stanza della casa frequentata da tutti;

• controllare con regolarità che cosa faccia il proprio figlio, condividendo con lui anche le attività sul computer;

• cercare di parlargli per capire quale genere di attività online gli piacciono;

• cercare online il suo nome: esaminando i suoi profili o i messaggi sui siti delle comunità di teenager, si può capire se è coinvolto in atti di bullismo.

INSEGNARE:

• mai dare informazioni personali, come nome, indirizzo, numero di telefono, età, nome e località della scuola o nome degli amici a chi non si conosce personalmente o a chi si conosce sul web;

• non condividere le proprie password, neanche con gli amici;

• non accettare incontri di persona con qualcuno conosciuto online;

• mai rispondere a un messaggio che faccia sentire confusi o a disagio. Meglio ignorare il mittente, terminare la comunicazione e riferire quanto accaduto a un adulto;

• mai usare un linguaggio offensivo o mandare messaggi volgari online.

ISTRUIRE A:

• non rispondere a e-mail o sms molesti e offensivi;

• non rispondere a chi insulta o prende in giro;

• non rispondere a chi offende nelle chat o esclude da una chat;

• salvare i messaggi offensivi che si ricevono (sms, mms, e-mail), prendendo nota del giorno e dell'ora in cui il messaggio è arrivato;

• cambiare il proprio nickname;

• cambiare il proprio numero di cellulare e comunicalo solo agli amici;

• utilizzare filtri per bloccare le e-mail moleste;

• non fornire mai dati personali (nome, cognome, indirizzo di residenza) a chi si conosce in chat o sul web;

• parlane immediatamente con un adulto (genitori o insegnanti);

• in caso di minacce fisiche o sessuali, è possibile contattare anche la Polizia.

QUESTIONARIO ANONIMO

Ti preghiamo di rispondere con sincerità a tutte le domande e di lavorare autonomamente senza commentarle con i compagni. Le risposte ai questionari sono confidenziali e non sarà mai possibile risalire al tuo nome, sei libero di rifiutarti di rispondere.

Se vorrai, dopo potremmo discutere del questionario insieme ai tuoi insegnanti.

Nessuno a scuola o a casa saprà in che modo hai risposto a queste domande.

Molte domande riguardano la tua vita a scuola dal momento in cui è **iniziata**, cioè a **partire da settembre**.

Quando rispondi cerca di pensare a tutto questo periodo e non soltanto agli ultimi giorni o mesi.

Ora puoi procedere.

Ti ringraziamo per la collaborazione.

BULLISMO e CYBERBULLISMO

Il Cyberbullismo (o bullismo elettronico) è una nuova forma di prepotenza che prevede l'utilizzo di e-mail, messaggi di testo (SMS), chat, siti web, telefoni cellulari o altre forme di informazione tecnologica allo scopo di tormentare, minacciare o intimidire qualcuno, diffondere dicerie e storie non vere sul conto di altri.

Il Cyberbullismo come il Bullismo, possono includere alcune azioni come minacce, insulti di diverso tipo e ripetuta umiliazione di qualcuno tramite supporto elettronico o a voce.

1) Conosci qualcuno che è ha subito prepotenze attraverso atti di Bullismo o Cyberbullismo in questo anno scolastico?

No ☐ Sì, fuori dalla scuola ☐

Sì, a scuola ☐ Sì, sia a scuola che fuori dalla scuola ☐

2) Hai mai subito prepotenze o azioni che ti hanno reso vittima o che ti abbiano fatto sentire a disagio in questo anno scolastico?

No ☐ Sì, dai compagni fuori dalla scuola ☐

Sì, dai compagni di scuola ☐ Sì, sia da compagni della scuola che da quelli fuori ☐

3) Quante volte è successo?

Mai ☐ Solo 1 volta ☐ 2-3 volte al mese ☐

1 volta a settimana ☐ Diverse volte alla settimana ☐

a.Mi sono arrivati brutti messaggi di testo SMS (facendo minacce e commenti) ☐

b.Foto/video offensivi sul cellulare ☐

c.Mi hanno fatto scherzi o telefonate mute ☐

d.Mi hanno inviato brutte e-mail ☐

e.Hanno diffuso riprese o foto di mie situazioni imbarazzanti o intime su internet o con il telefonino ☐

f.Hanno diffuso dicerie sul mio conto tramite web e/o SMS, MSN, FACEBOOK ☐

Anno scolastico	**Numero di segnalazioni**	**Numero di infrazioni**	**Numero di sanzioni disciplinari**

g.Ho ricevuto insulti sulla rete (MSN Messenger/Yahoo/FACEBOOK)

h.Altro(scrivi cosa):

4) Hai mai preso parte ad episodi di Bullismo e/o Cyberbullismo in questo anno scolastico?

No ☐ Qualche volta ☐ Spesso ☐

5) Sei a conoscenza che se vuoi, puoi segnalare atti di Cyberbullismo e Bullismo, utilizzando il servizio:

- Generazioni Connesse: http://www.generazioniconnesse.it/site/it/home-page/

SAFER INTERNET CENTRE - HELP LINE - CHAT

- Telefono Azzurro: 19696 (in forma anonima)

SI ☐ NO ☐

SCHEDA MONITORAGGIO ANNUALE BULLISMO E CYBERBULLISMO

Nell'ambito del monitoraggio e dell'implementazione della Policy di E-Safety si terranno in considerazione i dati annuali sulla base del seguente documento

Approvato dal Collegio Docenti del:

Nome del docente responsabile della sicurezza online (E-Safety Policy):

Schema riepilogativo delle situazioni gestite legate a rischi online

Scuola nella quale si è svolto episodio	**Data e ora episodio (riportato nelle schede segnalazione)**	**Riassunto episodio**	**Azioni intraprese**		**Insegnante con cui l'alunno si è confidato**	**Firma referente**
			Cosa?	**Da chi?**		