BSIC852002 - A14AA85 - REGISTRO PROTOCOLLO - 0000535 - 17/01/2024 - I.1 - U

# *E-Safety Policy*

INDICE DEI CONTENUTI

**1. Introduzione**

1. Scopo della *policy*.
2. Ruoli e responsabilità
3. Condivisione e comunicazione della *policy* all'intera comunità scolastica.
4. Gestione delle infrazioni alla *policy*.
5. Integrazione della *policy* con Regolamenti esistenti.

**2. Formazione e Curricolo**

1. Curricolo sulle competenze digitali per la componente studentesca.
2. Formazione del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica e sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

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

1. Accesso ad internet: filtri, antivirus e sulla navigazione.
2. Gestione accessi (password, backup,ecc.).
3. E-mail.
4. Sito web della scuola.
5. Socialnetwork.
6. Protezione dei dati personali.

**4. Strumentazione personale**

1. Per la componente studentesca: gestione degli strumenti personali - cellulari,tablet ecc..
2. Per il corpo docente e per il personale della scuola: gestione degli strumenti personali cellulari, tablet ecc.

**3. Prevenzione, rilevazione e gestione dei casi**

*Prevenzione*

- Rischi
- Azioni

*Rilevazione*

- Che cosa segnalare
- Come segnalare: con quali strumenti e a chi.
- Come gestire le segnalazioni.

*Gestione dei casi*

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

Firmato digitalmente da EMILIA PAGANO

# 1. INTRODUZIONE

## 1.1 Scopo della *policy*.

Questa *policy* si applica a tutti i membri della comunità scolastica che hanno accesso o che sono utenti dei sistemi informatici della scuola.

In particolare essa viene redatta per regolare il comportamento della componente studentesca dentro le aule scolastiche e per sensibilizzarla all'adozione di buone pratiche quando sono fuori dalla scuola e autorizza i membri del personale docente a erogare sanzioni disciplinari per comportamenti inappropriati avvenuti all'interno dell'istituzione scolastica. Questo è il caso degli episodi di cyber-bullismo come di altri fenomeni di cui si tratta nella presente politica, che possono avvenire al di fuori della scuola, ma che sono legati alla frequentazione della stessa.

L'Istituto comprensivo di Mazzano accoglie minori "nativi digitali" che fin dall'infanzia sono esposti a rischi di cui sono inconsapevoli, pertanto la scuola attua attività di prevenzione allo scopo di ridurre al minimo l'occorrenza di atti che non solo creano disagio nella comunità scolastica, ma possono configurarsi come reati.

La scuola opera in collegamento con le forze dell'ordine, con la Procura della Repubblica, con istituzioni del settore educativo, per mettere in campo strategie di prevenzione al cyber-bullismo e interventi di recupero nel caso in cui vengano individuati tali fenomeni, seguendo le norme del "Protocollo di prevenzione, intervento e contrasto dei fenomeni di bullismo e cyber-bullismo".

## 1.2 Ruoli e responsabilità

Dirigente Scolastico

Valuta l'efficacia della politica e ne monitora/indirizza l'attuazione, anche in collaborazione con personale scolastico, enti locali e *stakeholder* territoriali.

È responsabile della presentazione di questo documento all'attenzione del Consiglio di Istituto e al Collegio dei Docenti; deve anche valutare l'efficacia della politica e monitorarne/indirizzarne l'attuazione, anche in collaborazione con personale scolastico, enti locali e stakeholder territoriali. A tale scopo necessita di ricevere tempestive informazioni sulle violazioni al presente regolamento o eventuali problemi attualmente non noti dal corpo docente o dal personale ATA che ne sono a conoscenza

Animatore e Team digitale

Cura la redazione e la revisione annuale della *policy* sulla base delle osservazioni ricevute da tutti i soggetti interessati; ne assicura la massima diffusione dentro la comunità scolastica in tutte le sue componenti (docenti/ata, genitori e studenti), mediante pubblicazione sul sito della scuola. Si relaziona con la ditta che gestisce l'assistenza tecnico-informatica per definire le misure di sicurezza informatica più opportune; riferisce al Dirigente Scolastico situazioni o problemi di particolare rilevanza su cui intervenire.

Personale docente

Le insegnanti/gli insegnanti sono tenuti ad assicurare di:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- aver letto, compreso e sottoscritto la presente *policy*;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'animatore digitale per le opportune indagini / azioni /sanzioni;
- mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale

e realizzarle esclusivamente con sistemi ufficiali scolastici (registro elettronico, google suite…);
-far comprendere e mettere in pratica alla componente studentesca le regole di comportamento relative alla sicurezza informatica;
-far nascere nella componente studentesca una buona cognizione della proprietà del software e delle normative sul diritto d'autore nonché di far comprendere la necessità di effettuare ricerche sul web e la relativa estrazione di documenti evitando il plagio o l'illecita diffusione di dati personali;
-controllare l'uso dei dispositivi digitali nelle lezioni e nelle altre attività scolastiche che ne prevedono la necessità a scopi didattici;
-guidare la navigazione degli alunni, nelle lezioni in cui è previsto l'uso di Internet.

Personale ATA

Il personale ATA è tenuto ad assicurare di:
-avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
-aver letto, compreso e sottoscritto la presente *policy*;
-segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'animatore digitale per le opportune indagini / azioni / sanzioni;
-mantenere tutte le comunicazioni digitali con alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici;

Componente studentesca

Le alunne/gli alunni sono responsabili per l'utilizzo corretto dei sistemi informatici e della tecnologia digitale in accordo con i termini previsti da questa *policy*. In particolare sono tenuti a:
• non utilizzare dispositivi personali durante le attività didattiche se non espressamente consentito dal personale docente:
• avere una buona comprensione delle possibilità di ricerca sul web e della necessità di evitare il plagio, rispettare le normative sul diritto d'autore, non diffondere dati personali;
• comprendere l'importanza della segnalazione di ogni abuso, uso improprio o accesso a materiali inappropriati e conoscere il protocollo per tali segnalazioni;
• conoscere e comprendere le politiche sull'uso di dispositivi mobili e di macchine fotografiche digitali; capire le politiche di utilizzo delle immagini ed essere consapevoli del significato e della gravità del cyber-bullismo.
• capire l'importanza di adottare buone pratiche di sicurezza informatica in tutti i momenti della vita, a tutela dell'incolumità propria e altrui e per evitare di perpetrare reati punibili a qualsiasi livello (da quello scolastico fino all'intervento della Magistratura).

Genitori

Genitori e tutori svolgono un ruolo cruciale nel garantire che i loro figli comprendano la necessità di utilizzare i dispositivi digitali in modo appropriato. La scuola coglierà ogni occasione per sensibilizzare i genitori circa questi problemi attraverso incontri con esperti, circolari, sito web e altre comunicazioni telematiche. I genitori saranno incoraggiati a sostenere la scuola nel promuovere le buone pratiche di *e- safety* e a seguire le linee guida sull'uso appropriato di:
• immagini digitali e video registrati in occasione di eventi scolastici, anche al di fuori delle aule;
• accesso alle sezioni del sito dedicate ai genitori, con particolare riguardo al registro elettronico;

• dispositivi personali dei loro figli.

1.3 Condivisione e comunicazione della *policy* all'intera comunità scolastica.

Per evitare che l'adozione di questa *policy* rappresenti un mero atto formale, l'Istituto si impegna a prendere spunto da essa come base di partenza per una serie di azioni e iniziative. A partire dalla pubblicazione sul sito della scuola:

- Per il corpo docente, discussione collegiale sui contenuti, sulle pratiche indicate e su come inserire nel curricolo le tematiche di interesse della *policy*; un confronto collegiale, su base annuale, circa la necessità di apportare modifiche e miglioramenti alla *policy* vigente; elaborazione di protocolli condivisi di intervento.
- Per la componente studentesca, la discussione in classe della *policy* nei primi giorni di scuola.
- Per i genitori, l'organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare.

1.4 Gestione delle infrazioni della *policy*.

Le infrazioni alla policy possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori a docenti/ATA.

Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. Infatti è bene ricordare a tutti che nel momento in cui un qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia (ex art. 331 del codice di procedura penale). L'omissione di denuncia costituisce reato (art. 361). I reati che, in ambiente scolastico, possono essere riferiti all'ambito digitale e commessi per via telematica sono tra gli altri:

-*Minaccia*; in particolare, se la minaccia è grave, per tale reato si procede d'ufficio (art. 612 cod. pen.);
-*Induzione alla prostituzione minorile* (art. 600*bis*);
-*Pedopornografia* (art. 600*ter*);
-*Corruzione di minorenne* (art. 609*quinquies*).

Per i reati sessuali la magistratura di norma procede su querela di parte; tuttavia nei casi più gravi si persegue d'ufficio e in genere i reati verso le/i minori sono tra quelli per i quali si procede d'ufficio.

Nel caso in cui le infrazioni della *policy* violino norme previste dal Regolamento di Istituto si procede secondo quanto previsto dal Regolamento stesso; qualora le infrazioni riguardino l'opportunità di certi comportamenti o la convivenza civile, la scuola eroga delle sanzioni secondo il principio della sensibilizzazione e del risarcimento dell'eventuale danno provocato, in uno spirito di recupero e rieducazione.

1.5 Integrazione della *policy* con Regolamenti esistenti.

La presente *policy* è allegata in appendice al Regolamento di Istituto ed è strettamente collegato al Regolamento del Registro Elettronico, al Regolamento per l'utilizzo della Google Workspace, al Protocollo di prevenzione, intervento e contrasto del bullismo e cyber-bullismo e al Regolamento per la tutela della Privacy.

## 2. FORMAZIONE E CURRICOLO

### 2.1 Curricolo sulle competenze digitali per la componente studentesca.

Le TIC e Internet sono un elemento essenziale nella vita del XXI secolo. La scuola ha il dovere di fornire alla componente studentesca l'accesso a questi strumenti come parte della loro esperienza di apprendimento e di far maturare in loro le competenze per una proficua cittadinanza digitale. L'uso delle TIC va inserito pertanto nel curricolo sia a livello disciplinare sia a livello interdisciplinare.

In particolare il curricolo dovrà essere strutturato per prevedere di:

- insegnare ciò che è accettabile nell'utilizzo di Internet e ciò che è vietato, fornendo strumenti per l'utilizzo efficace di Internet e la conoscenza delle conseguenze delle violazioni;
- mostrare come produrre, pubblicare e presentare contenuti digitali in modo appropriato, sia in ambienti privati sia per un pubblico più vasto;
- impiegare materiali prelevati da Internet a scopi didattici conformemente al diritto d'autore;
- rendere alunne e alunni criticamente consapevoli dei materiali che si leggono sul web allo scopo di vagliare le informazioni prima di accettarne la fondatezza, la coerenza, le origini;
- mostrare la segnalazione di contenuti Internet sgradevoli o illegali.

### 2.2 Formazione del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica e sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

La formazione del corpo docente verrà organizzata su due livelli: interno ed esterno. A livello interno, nel PTOF si prevede che una parte della formazione in servizio obbligatoria ai sensi della L. 107/2015 sia dedicata proprio all'uso e all'inserimento delle TIC nella didattica e ai temi informatici in generale. Tale formazione è svolta da docenti dell'Istituto che fanno parte del team digitale, per cui il MIUR prevede opportuni percorsi la cui ricaduta viene annualmente tarata secondo le esigenze formulate dal Collegio Docenti, ed è improntata alla condivisione di esperienze significative e di buone pratiche.

Per quanto riguarda la formazione esterna, la scuola assicura tempestiva e capillare informazione su corsi, convegni e seminari che riguardino tali argomenti, cercando altresì di agevolare il personale che intenda parteciparvi. Infine la scuola può aderire a progetti appositi di formazione presentati da enti e associazioni, come già avvenuto in passato.

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

### 3.1 Accesso ad internet: filtri, antivirus e sulla navigazione.

L'assistenza tecnica esterna di cui si avvale l'Istituto ha già da parecchi anni configurato un *proxy server* per monitorare il traffico web e per bloccare l'accesso a siti inappropriati a un contesto scolastico. Occorre invece sensibilizzare tutta la comunità scolastica sull'opportunità di mantenere aggiornati gli antivirus installati sulle macchine personali e controllare i dispositivi di archiviazione esterna che vengano collegati al proprio pc.

3.2 Gestione accessi.

L'Istituto attualmente è dotato di una rete wireless, fornita dall'Amministrazione Comunale, destinata al solo utilizzo didattico da parte del corpo docente.

Ai docenti è consentito accedere ad Internet dai propri dispositivi utilizzando la rete Wi-Fi dell'Istituto, secondo gli usi consentiti. L'Istituto intende mantenere un *log* corrente sull'uso dei sistemi della scuola per la verifica di eventuali violazioni della *policy,* oltre che delle leggi vigenti, da parte di chiunque abbia accesso a essi.

3.3 E-mail.

L'Istituto fornisce una casella di posta elettronica @icmazzano.edu.it a tutto il personale docente e ATA e ad alunni/genitori.

Sulla rete scolastica tutti sono invitati a utilizzare solo account di posta elettronica presenti nel dominio scolastico e per scopi inerenti lo svolgimento didattico/organizzativo.

Le comunicazioni tra personale scolastico, famiglie e allieve/allievi via e-mail devono avvenire tramite l'indirizzo e-mail della scuola o all'interno della piattaforma di apprendimento, per consentire l'attivazione di protocolli di controllo.

E-mail in arrivo da mittenti sconosciuti vanno trattate come sospette ed eventuali allegati non devono essere aperti.

3.4 Sito web della scuola.

I dati di contatto dell'Istituto sono reperibili sul sito web https://icmazzano.edu.it.

Il sito prevede un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali, avvisi di carattere generale.

Il personale che è in possesso delle credenziali per la gestione dei contenuti sul portale si assumerà la responsabilità editoriale di garantire che il contenuto inserito sia accurato e appropriato.

3.5 Social Network.

La scuola e l'Amministrazione Comunale sono in grado di controllare l'accesso ai siti di social networking attraverso i *log* del *proxy server;* nella pratica didattica si cerca di educare la componente studentesca al loro uso sicuro. Per esempio a ogni utente sarà consigliato di non fornire mai dati personali di alcun tipo che possano identificare con precisione le persone e la loro residenza o ubicazione.

La componente studentesca non deve pubblicare senza permesso foto personali proprie o altrui su qualsiasi spazio di social network previsto nella piattaforma di apprendimento scolastico. Alunne/alunni, genitori e personale docente/ATA saranno informati sull'uso sicuro degli spazi di social network e sulle conseguenze legali di ogni uso improprio.

3.6 Registro elettronico.

Ogni famiglia riceve le credenziali per l'accesso riservato al registro elettronico, in cui il corpo docente è tenuto a registrare assenze, valutazioni, note e osservazioni. L'uso del registro elettronico è spiegato alle famiglie nel corso del primo consiglio di classe dell'anno scolastico e la pubblicazione delle informazioni attraverso tale strumento assolve l'obbligo di comunicare prontamente ed efficacemente ogni evento riguardante l'alunno/a. Coloro che non possono accedere a Internet e di conseguenza non possono consultare il registro elettronico sono pregati di darne segnalazione al coordinatore del consiglio di classe, che verificherà la trascrizione delle comunicazioni sul diario e la firma dei genitori. Per un approfondimento e regole precise si veda l'apposito regolamento.

3.7 Protezione dei dati personali.

Si fa riferimento a tutto quanto previsto dal *Decreto legislativo 30 giugno 2003, n. 196* (c. d. Codice della Privacy). Tuttavia, si possono individuare al riguardo alcune linee guida di *e-safety*: il personale non deve condividere numeri di telefono personali o indirizzi di posta elettronica privati con la componente studentesca e con i genitori. Un telefono o una e-mail della scuola sarà fornito al personale cui è richiesto il contatto con la componente studentesca o con i genitori.

Le fotografie o i video da pubblicare sul sito che includano allieve e allievi saranno selezionati con cura e non permetteranno a singoli di essere chiaramente identificati a meno che non si tratti di eventi particolari per cui le famiglie potranno concedere opportuna autorizzazione. La scuola cercherà di utilizzare fotografie o video di gruppo piuttosto che foto integrali di singoli.

All'atto dell'iscrizione è richiesto alle famiglie di prendere visione dell'informativa riguardante l'uso dell'account e delle immagini/video delle/dei minori secondo i principi sopra indicati. Ogni caso particolare sarà preso in considerazione per stabilire l'opportunità di pubblicare dati personali e sarà presentata apposita richiesta circostanziata che varrà solo per lo specifico evento.

4. STRUMENTAZIONE PERSONALE

4.1 Per la componente studentesca.

I telefoni cellulari, i tablet e le relative fotocamere e registratori vocali non verranno utilizzati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate dal corpo docente o per esigenze personali certificate dagli organi competenti.

Nella scuola primaria si chiede alle famiglie di non lasciare tali dispositivi ad alunne e alunni.

Per gli alunni con bisogni educativi speciali (DSA - BES) si adotteranno le modalità di impiego di strumenti compensativi quali tablet e computer portatili previsti all'interno del PDP.

Giochi e console non sono consentiti. Saranno requisiti dal docente che ravvisa l'infrazione, depositati nella cassaforte della segreteria e consegnati al genitore/tutore convocato, che sarà contestualmente informato dell'eventuale sanzione disciplinare comminata al trasgressore.

Nel caso in cui debbano comunicare con la famiglia durante l'orario scolastico, alunne e alunni possono usare gratuitamente la linea fissa della scuola rivolgendosi a un collaboratore; allo stesso modo le famiglie devono chiamare il numero della scuola di appartenenza se hanno assoluta necessità di parlare con i propri figli. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.

L'invio di materiali abusivi, offensivi o inappropriati è vietato, anche se avviene all'interno di cerchie o gruppi di discussione privati.

4.2 Per il personale docente/ATA.

Il personale preferirà, quando ciò è possibile, l'impiego della strumentazione fornita dalla scuola rispetto a quella personale (portatili, pc fissi, …); le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali. Telefoni cellulari, tablet, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate o per scopi lavorativi.

La password di accesso alla rete wireless va custodita con cura e per nessuna ragione deve essere divulgata a chi non ha titolo per utilizzarla (studenti, genitori, operatori esterni). L'uso improprio della rete è contestato al titolare delle credenziali con cui è avvenuta la comunicazione.

Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (chiavette usb, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.

5. PREVENZIONE E RILEVAZIONE DEI CASI

Le misure di prevenzione comprendono l'integrazione nel curricolo dei temi legati al corretto utilizzo delle TIC e di Internet.

La scuola si avvale della collaborazione di enti e associazioni per realizzare incontri rivolti alla componente studentesca e alle famiglie con l'intento di fornire ogni elemento utile alla prevenzione e alla gestione dei problemi relativi alla sicurezza informatica; le famiglie sono invitate a proporre tematiche di particolare interesse su cui la scuola focalizzerà il proprio intervento.

L'Istituto comprensivo attiva inoltre uno sportello di ascolto al quale la componente studentesca si può rivolgere per avere consigli e sostegno psicologico anche relativamente alle tematiche del cyber-bullismo.

La rilevazione dei casi è compito dell'intera comunità educante.

La gestione dei casi rilevati va differenziata a seconda della loro gravità; fermo restando che è opportuna la condivisione a livello di Consiglio di Classe di ogni episodio rilevato, anche minimo, alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe. Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e come rimediare. Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico come intervenire.

Firmato digitalmente da EMILIA PAGANO