ISTITUTO COMPRENSIVO STATALE "CENTRO STORICO"
Scuola dell'infanzia, primaria e secondaria di primo grado
Largo A. Gramsci, 3/4 – 47921 RIMINI (RN)
Telefono: 0541.78.23.75 Fax: 0541.78.47.96
Codice MIUR: RNIC817007 - C.F. 91142610400
C.FATT.PA: UFLU42 - C.IPA: icics_0
PEC: rnic817007@pec.istruzione.it E-MAIL: rnic817007@istruzione.it
SITO: www.centrostorico.gov.it

Unione Europea
FONDI STRUTTURALI EUROPEI
PON 2014-2020
PER LA SCUOLA - COMPETENZE E AMBIENTI PER L'APPRENDIMENTO (FSE-FESR)
MIUR
Ministero dell'Istruzione, dell'Università e della Ricerca
Dipartimento per la programmazione e la Gestione delle Risorse Umane, Finanziarie e Strumentali
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

Z:\Regolamenti\0043 linee sicurezza informatica e-safety policy vers 1.1.doc

Prot. vedi segnatura

Linee di condotta per la sicurezza informatica (E-SAFETY POLICY) vers. 1.1

Lo scopo delle **Linee di condotta per la sicurezza informatica (E-SAFETY POLICY)** è:

- stabilire i principi fondamentali a cui si devono attenere tutti i membri della comunità scolastica per quanto riguarda l'utilizzo di tecnologie;
- salvaguardare e proteggere i bambini, i ragazzi e il personale dell'Istituto da violazioni e reati connessi con l'utilizzo della rete e delle strumentazioni elettroniche;
- promuovere nel personale della scuola modalità di lavoro sicuro e responsabile con le tecnologie elettroniche e digitali di comunicazione e monitorare gli standard e le prassi;
- impostare un codice di comportamento per un uso responsabile di internet a scopo didattico, personale o ricreativo;
- affrontare gli abusi messi in atto online.

Principi generali

Scuola e famiglia possono essere determinanti nella diffusione di un atteggiamento mentale e culturale che consideri la diversità come una ricchezza, promuova l'accettazione, la consapevolezza dell'altro, lo sviluppo del senso della comunità e della responsabilità collettiva.

Per definire una strategia ottimale di prevenzione e di contrasto ai comportamenti-problema favoriti dal web, le esperienze e le conoscenze acquisite e prodotte vanno contestualizzate alla luce dei cambiamenti che hanno profondamente modificato la società sul piano etico, sociale e culturale; ciò comporta una valutazione ponderata delle procedure adottate, per assicurarne l'efficacia. Si ricordano qui di seguito alcuni principi generali per l'utilizzo consapevole del web:

1. internet favorisce la libertà di espressione e, quando si entra a far parte di una community o di un servizio dove interagiscono più utenti, vanno considerati abusi meritevoli di segnalazione solo quei contenuti palesemente impropri o illeciti e non tutto ciò con cui semplicemente non si è d'accordo o non piace;
2. quando si inizia a navigare tra i servizi dei social network e le applicazioni web è necessario informarsi subito su quali sono i diritti e i doveri dell'utente, leggendo il regolamento, tenendosi aggiornati, esplorando i siti informativi e istituzionali che affrontano queste tematiche;
3. se si condividono informazioni personali, bisogna farlo scegliendo con cura che cosa rendere pubblico e cosa rendere privato. E' indispensabile scegliere con attenzione le amicizie con cui accrescere la propria rete e i gruppi a cui aderire, proteggendo la propria identità digitale con password complesse e usando una domanda di recupero password dalla risposta non banale;
4. se si condividono, come privati, elementi multimediali o informazioni che riguardano più persone è necessario avere il permesso di ciascun utente coinvolto prima di effettuare la pubblicazione. Se invece la condivisione avviene in qualità di ente pubblico (es. docenti nell'adempimento della loro funzione) è necessaria una previsione di legge;
5. bisogna contribuire a rendere il web un luogo sicuro, pertanto ogni volta che un utente commette involontariamente un abuso o un errore, pubblicando del materiale illecito non idoneo o offensivo, è opportuno contattarlo e fornire le spiegazioni relative alle regole, diffondendo così i principi della sicurezza.
6. ogni abuso subìto rilevato nella navigazione deve essere segnalato tramite gli strumenti offerti dal servizio, indicando in modo semplice i riferimenti per ottenere tempestivamente la rimozione del contenuto. Tutti i social network garantiscono la possibilità di segnalare materiali inopportuno mediante semplici operazioni da compiere direttamente sul sito: è quindi opportuno, prima di denunciare un incidente o una "bravata" alle autorità competenti, avvalersi della modalità di segnalazione che talvolta può risolvere il problema senza obbligare le parti in causa ad incorrere in lunghe conseguenze giudiziarie.

Le principali aree di rischio

Le principali aree di rischio per la nostra comunità scolastica, in considerazione dell'età degli studenti e delle pratiche amministrative e didattiche usuali, possono essere considerate le seguenti:

- esposizione a contenuti on line inappropriati;
- difficoltà di validazione dei contenuti e di verifica della loro veridicità, esattezza, appropriatezza;
- atteggiamenti e contenuti di odio e/o di intolleranza;
- fenomeni di adescamento;
- cyberbullismo, stalking, sexting;
- furto di identità, appropriazione ed uso delle credenziali di altri;

- violazione della privacy (es: diffusione di informazioni personali);
- danneggiamento della reputazione online;
- rischi per la salute e benessere (es. in relazione al tempo speso online su internet o giochi);
- violazione delle normative sul copyright.

Ruoli e responsabilità: che cosa ci si aspetta dagli attori della comunità scolastica

Ruolo	**Responsabilità**
Il dirigente scolastico	❑ Ha la responsabilità generale per la sicurezza dei dati ❑ Mette in atto strategie a garanzia che la scuola utilizzi un internet service filtrato, approvato e conforme ai requisiti di legge vigenti ❑ Ha la responsabilità di assicurare che il personale riceva una formazione adeguata ❑ Individua procedure da seguire in caso di infrazione della e-safety policy ❑ Ha il compito di definire e rivedere periodicamente la e-Safety policy ❑ Prevede azioni di monitoraggio periodiche della sicurezza online
I responsabili della sicurezza online	❑ Promuovono la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica ❑ Prevedono l'inserimento dell'educazione alla sicurezza online nel programma di studi ❑ Forniscono a tutto il personale informativa sulle procedure che devono essere seguite in caso di incidente per la sicurezza online ❑ Garantiscono che sia tenuto un registro di incidenti di sicurezza online ❑ Promuovono la formazione e la consulenza per tutto il personale ❑ Mettono in atto azioni di coordinamento con le autorità locali e le agenzie competenti ❑ Predispongono azioni di controllo ❑ Dispongono la pubblicazione della e-safety Policy sul sito della scuola
L'animatore digitale e il team digitale	❑ Diffondono la conoscenza della e-safety Policy tra i colleghi
Gli insegnanti	❑ Curano l'inserimento delle tematiche legate alla sicurezza online nel programma di studi ❑ Forniscono supervisione e guida agli alunni quando sono impegnati in attività di apprendimento che coinvolgano la tecnologia online ❑ Operano affinché gli alunni sviluppino la consapevolezza dei rischi legati all'uso didattico del web (modalità di ricerca, validazione dei contenuti ecc.)
Tutto il personale scolastico	❑ Fornisce il proprio contributo alla promozione delle politiche di sicurezza elettronica e digitale ❑ Acquisisce consapevolezza dei problemi di sicurezza online connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili ❑ Contribuisce al monitoraggio sull'uso di dispositivi tecnologici e all'attuazione delle politiche scolastiche relative a questi dispositivi ❑ Segnala qualsiasi sospetto abuso o problema al responsabile della sicurezza online ❑ Dà comunicazione scritta al dirigente circa il furto o lo smarrimento delle credenziali d'accesso ai servizi informatici della scuola come il registro elettronico, il SIDI, il portale di presa visione delle circolari e di invio delle pratiche personali (Argo, Nuvola, Google Apps ecc...) e gli altri gestionali utilizzati per l'amministrazione e la didattica, provvedendo a modificare immediatamente le password in questione. Tale comunicazione va fatta anche in caso di furto o smarrimento di tablet/cellulari/pc/notebook o altri strumenti personali su cui potrebbero essere stati salvati, anche inavvertitamente, i codici degli account sopradescritti ❑ Mette in atto comportamenti sicuri, responsabili e professionali nell'uso della tecnologia ❑ Garantisce che le comunicazioni digitali con gli studenti e con le famiglie siano a livello professionale ed esclusivamente attraverso i sistemi previsti dall'Istituzione scolastica
Gli alunni	❑ Conoscono e comprendono la e-safety policy ❑ Comprendono l'importanza di segnalare abusi o l'uso improprio delle strumentazioni elettroniche e del web ❑ Si rivolgono agli insegnanti e ai genitori nel caso in cui essi stessi o qualcuno che conoscono si senta preoccupato e vulnerabile quando utilizza la tecnologia online ❑ Conoscono, comprendono e rispettano le regole relative all'uso dei telefoni cellulari e di altri dispositivi portatili ❑ Conoscono e comprendono le linee della scuola sull'uso delle immagini ❑ Comprendono l'importanza di adottare buone pratiche di sicurezza online quando si usano le tecnologie digitali anche fuori dalla scuola

I genitori	❑ Sostengono la scuola nel promuovere la sicurezza online ❑ Leggono, comprendono e accettano le disposizioni di e-safety Policy ❑ Consultano il sito web, il registro elettronico e gli altri spazi online della scuola in conformità con quanto stabilito dalla stessa ❑ Verificano che la scuola abbia preso tutte le precauzioni necessarie circa un uso corretto della tecnologia da parte degli alunni e segnalano tempestivamente eventuali situazioni di criticità di cui vengano a conoscenza

La scuola si riserva di limitare l'accesso e l'uso della rete interna ed esterna secondo i normali canali di protezione presenti nei sistemi operativi e si organizza per evitare comportamenti che non rientrino nelle norme o nelle linee guida condivise, quali ad esempio:

- ➔ scaricare file video musicali protetti da copyright;
- ➔ visitare siti non necessari ad una normale attività didattica;
- ➔ alterare i parametri di protezione dei computer in uso;
- ➔ utilizzare la rete per interessi privati e personali che esulano dalla didattica o dall'attività amministrativa;
- ➔ violare le leggi sul diritto d'autore;
- ➔ navigare su siti non accettati dalla protezione interna.

Disposizioni e procedure:
Si elencano le principali procedure che dovranno essere messe in atto a garanzia della sicurezza informatica e digitale degli alunni e del personale della scuola:

- ❖ il sistema è periodicamente controllato dagli incaricati;
- ❖ la scuola può verificare periodicamente i file utilizzati, i file temporanei e i siti visitati da ogni postazione;
- ❖ la scuola può archiviare i tracciati del traffico internet;
- ❖ è vietato installare o scaricare da internet software non autorizzati;
- ❖ al termine di ogni collegamento il browser deve essere chiuso e al termine del lavoro quotidiano il computer deve essere spento;
- ❖ periodicamente sono condotte verifiche antivirus sui computer e sull' unità di memorizzazione di rete;
- ❖ l'utilizzo di CD e chiavi USB personali degli alunni deve essere autorizzato dal docente;
- ❖ le chiavi USB, anche di proprietà dei docenti, possono essere utilizzate solo previa scansione antivirus;
- ❖ la scuola si riserva di limitare il numero di siti visitabili e le operazioni di download;
- ❖ il materiale didattico dei docenti può essere messo in rete, anche su siti personali, sempre esclusivamente nell'ambito del presente regolamento e nel rispetto delle leggi.

Sito web
L'istituto dispone di un proprio spazio web e di un proprio dominio e gestisce un proprio sito web nello spazio di proprietà.
La gestione del sito web della scuola e la rispondenza alle normative per quanto concerne i contenuti (accuratezza, appropriatezza, aggiornamento) e le tecniche di realizzazione e progettazione sono a cura del webmaster.
La scuola detiene i diritti d'autore dei documenti che si trovano sul proprio sito o di quei documenti per i quali è stato chiesto ed ottenuto il permesso dall'autore proprietario.
Le informazioni pubblicate sul sito della scuola relative alle persone rispettano le norme vigenti sulla privacy.
La scuola, in qualità di Ente pubblico, diffonde sul proprio sito web esclusivamente i contenuti che saranno valutati come pertinenti alle finalità istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale secondo le disposizioni normative.

Sicurezza della rete
L'istituto dispone di una rete di segreteria cui accedono i computer dell'amministrazione, isolati dal resto della rete di istituto (rete didattica).
Il collegamento di computer portatili o palmari personali alla rete di istituto deve essere autorizzato dal dirigente scolastico.
La rete internet è protetta da firewall e le postazioni sono protette con sistemi antivirus regolarmente aggiornati.
La memorizzazione dei documenti e delle impostazioni personali è sconsigliabile sulle postazioni legate alla didattica e di conseguenza utilizzate da più utenti. Su tali dispositivi non è garantito il servizio di backup, pertanto si consiglia di fare copia dei propri documenti e dati su un supporto personale oppure, preferibilmente, di salvare i propri documenti in uno spazio Cloud.
L'istituto dispone di una rete con tecnologia senza fili; l'accesso alla rete wireless è regolato da un controller che determina l'accesso degli utenti tramite il riconoscimento del dispositivo utilizzato. L'ottenimento delle credenziali è riservato al personale dell'Istituto ed eventuali ospiti e le regole di comportamento sono analoghe a quelle per la connessione alla rete cablata dell'Istituto.

Strumentazione personale
Come da regolamento di istituto agli studenti è vietato l'utilizzo del cellulare per uso personale all'interno della scuola; qualunque tipo di dispositivo personale potrà essere utilizzato esclusivamente per ragioni didattiche e previa autorizzazione del docente.

I docenti e tutto il personale della scuola possono utilizzare dispositivi personali a scopo didattico o amministrativo, secondo le indicazioni su esposte per il collegamento alla rete; gli usi a scopo personale sono consentiti esclusivamente al di fuori dell'orario lavorativo.

Gestione delle infrazioni alla e-policy

La scuola si impegna ad adottare tutte le precauzioni necessarie per garantire la sicurezza online, nei limiti delle proprie prerogative e delle proprie possibilità di investimento economico; tuttavia data la complessità delle tecnologie e la velocità dei cambiamenti nell'ambito digitale, risulta difficile garantire in questo settore una sicurezza totale, per la quale devono impegnarsi a contribuire tutti i componenti della comunità scolastica.

In caso di infrazioni si procederà secondo le seguenti linee di condotta:

- chiunque venga a conoscenza di una possibile infrazione, volontaria o involontaria, delle regole condivise, è tenuto ad informarne tempestivamente i responsabili della sicurezza;
- l'alunno coinvolto o a conoscenza di eventi di cyberbullismo, di violazione della privacy ecc. informerà immediatamente i docenti e/o i propri genitori;
- il docente informato dagli alunni provvederà a:
    - mettere in atto immediatamente le possibili misure di salvaguardia e riduzione del danno (es. immediato cambio password in caso di furto credenziali ecc.);
    - informare tempestivamente il dirigente dell'evento;
- il dirigente scolastico, supportato dai responsabili, attiverà ricerche volte a verificare gli eventi e la loro gravità;
- nel caso di coinvolgimento diretto degli alunni, in qualità di agenti o di vittime dell'evento, il dirigente convocherà al più presto i genitori per metterli al corrente e concordare strategie comuni di intervento;
- in accordo con i responsabili, il dirigente provvederà a programmare ogni possibile intervento di tipo tecnico ed organizzativo volto a sanare la situazione individuata e a prevenirla per il futuro;
- in considerazione del grado di gravità dell'evento, il dirigente valuterà la possibilità di sanzioni disciplinari per il personale della scuola e/o per gli alunni responsabili. In casi di possibile rilevanza penale, il dirigente inoltrerà segnalazione alle autorità competenti.

A titolo esemplificativo, si considerano infrazioni passibili di sanzione per gli studenti:

- la consultazione di siti non educativi durante le lezioni;
- l'utilizzo non autorizzato di email, chat, social durante le attività didattiche;
- l'uso non autorizzato del telefono cellulare o di altre nuove tecnologie durante le lezioni;
- l'uso e/o la diffusione di materiale offensivo verso compagni o docenti, anche se praticato in orario diverso da quello scolastico;
- la messa in atto di procedure finalizzate a danneggiare o distruggere deliberatamente i dati di qualcuno o alla violazione della privacy altrui;
- la trasmissione o la pubblicazione di materiale che violi i diritti d'autore o le leggi sulla privacy;
- comportamenti atti a screditare la scuola sul web;
- danni intenzionali all'hardware o al software.

Relativamente al personale scolastico

- uso di internet per attività personali non legate allo sviluppo professionale;
- utilizzo di supporti di memorizzazione dei dati personali in modo non adeguato;
- mancata implementazione delle adeguate procedure di salvaguardia;
- qualsiasi comportamento sul web che comprometta la professionalità del personale nella scuola e nella comunità o l'immagine della scuola;
- uso improprio di primo livello di sicurezza dei dati (ad es. uso illecito di password);
- violazione del copyright o della licenza per l'installazione di software;
- danni intenzionali all'hardware o al software;
- qualsiasi tentativo deliberato di violare la protezione dei dati o la sicurezza Informatica.

Disposizioni finali.

La e-safety Policy sarà riesaminata annualmente o quando si verificano cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola.

Nell'ambito della revisione della e-safety Policy tutte le versioni saranno memorizzate per eventuali controlli sulla base del seguente documento:

Versione	1.1 (in carattere sottolineato le modifiche rispetto alla versione precedente)
Data	Vedi segnatura
Autore	Il dirigente scolastico Lorella Camporesi