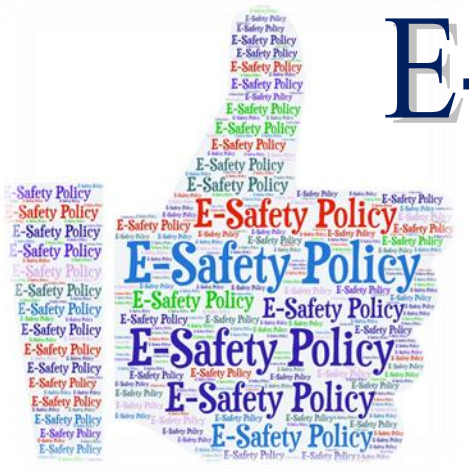
Codice MIUR RAIC829007 - C.F. 92082630390
Via Caduti per la Libertà, 16 - 48015 CERVIA (RA) - tel.0544/71955 fax 0544/72246
E mail: raic829007@istruzione.it - Pec: raic829007@pec.istruzione.it
web: www.iccervia2.gov.it



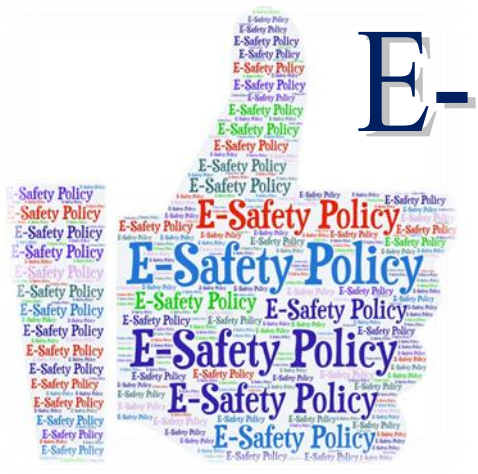
E-Safety Policy

Istituto Comprensivo Cervia 2

INDICE DEI CONTENUTI

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

Codice MIUR RAIC829007 - C.F. 92082630390
Via Caduti per la Libertà, 16 - 48015 CERVIA (RA) - tel.0544/71955 fax 0544/72246
E mail: raic829007@istruzione.it - Pec: raic829007@pec.istruzione.it
web: www.iccervia2.gov.it



E-Safety Policy

Istituto Comprensivo Cervia 2

1. INTRODUZIONE

Nell'ambito del progetto "Generazioni connesse" (www.generazioniconnesse.it) al quale la scuola ha aderito nel 2015, l'Istituto ha elaborato delle **linee guida per il corretto uso** della rete e delle strumentazioni informatiche (**E-Safety Policy**).
Non si tratta di un documento meramente formale, poiché a partire da esso la scuola intende promuovere:

- la **formazione** rivolta al personale interno circa le tematiche previste dalla *policy*;
- l'**impegno** di tutti gli attori coinvolti nel rispetto di quanto definito nel documento;
- l'**adeguamento del curricolo** per ottemperare a quanto stabilito nella *policy*;
- la **sensibilizzazione** dei genitori sul tema della sicurezza online;
- dei **partenariati** con enti e associazioni esterne.

Il nostro Istituto, particolarmente attento alle tematiche dell'educazione alla legalità, della sicurezza sul web, del bullismo e del cyberbullismo, attivo nella collaborazione alle iniziative della Settimana della Salute Digitale, ha adottato questo **protocollo di E-Safety Policy**, anche nell'ottica della adozione delle misure minime di sicurezza ICT (Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015, pubblicate in Gazzetta Ufficiale il 07 aprile 2017) cui si sta progressivamente adeguando, al fine di innalzare il proprio livello di sicurezza informatica.

1.1. Scopo della E-Safety Policy

Il documento ha lo scopo di informare l'utenza per un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente. In particolare l'intento della scuola è quello di promuovere l'uso consapevole e critico da parte degli alunni delle tecnologie digitali e di internet, di far acquisire loro procedure e competenze "tecniche", ma anche corrette norme comportamentali, di prevenire ovvero rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali. Gli utenti, siano essi maggiorenni o minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto la Scuola promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti. In questo contesto, gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose.

L'Istituto comprensivo Cervia2 accoglie minori "nativi digitali" che fin dall'infanzia sono esposti a rischi di cui sono inconsapevoli, pertanto la scuola attua parallelamente attività di prevenzione, controllo e formazione di allieve, allievi e famiglie 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 stretto collegamento con le forze dell'ordine, con la Procura della Repubblica e con istituzioni del settore educativo, per mettere in campo strategie di prevenzione al cyberbullismo e interventi di recupero nel caso in cui vengano individuati tali fenomeni, informando i genitori/tutori e chiedendo la loro collaborazione anche qualora gli episodi si siano verificati al di fuori delle attività didattiche.

1.2. Ruoli e Responsabilità

(che cosa ci si aspetta da tutti gli attori della Comunità Scolastica)

RUOLO	RESPONSABILITÀ
Il Dirigente Scolastico	Il ruolo della Dirigente Scolastica nel promuovere l'uso corretto e consapevole delle tecnologie e di internet include i seguenti compiti: - garantire la sicurezza (tra cui la sicurezza online) dei membri della comunità scolastica; - garantire che tutti le/i docenti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a, delle differenze e un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della Comunicazione (TIC); - comprendere e seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli/alle alunni/e nell'utilizzo delle TIC a scuola.

Il Direttore dei Servizi generali e amministrativi	Il ruolo del direttore dei servizi generali e amministrativi include i seguenti compiti: - assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni; - garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli/delle alunni/e per la notifica di documenti e informazioni della Dirigente Scolastica e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.
L'Animatore Digitale ed il suo Team	Compiti dell'Animatore Digitale e del suo Team: - stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale", fornire consulenza e informazioni al personale in relazione ai rischi online e alle misure di prevenzione e gestione degli stessi; - monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola; - assicurare che l'utente possa accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione); - coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".
Il referente del "Bullismo e Cyberbullismo"	- Promuove la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale; - coordina le attività di prevenzione ed informazione sulle sanzioni previste e sulle responsabilità di natura civile e penale, anche con eventuale affiancamento di genitori e studenti; - si rivolge a partner esterni alla scuola, quali servizi sociali e sanitari, aziende del privato sociale, forze di polizia,… per realizzare un progetto di prevenzione; - cura rapporti di rete fra scuole per eventuali convegni/seminari/corsi e per la giornata mondiale sulla Sicurezza in Internet, la "Safer Internet Day".
I Docenti	Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti: · informarsi/aggiornarsi sulle problematiche attinenti alla sicu-

	rezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento; · garantire modalità di utilizzo corretto e sicuro delle TIC e di internet (anche da parte degli alunni); · assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente; · nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei; - segnalare alla Dirigente Scolastica e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli/delle alunni/e in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.
Il Personale scolastico	Il ruolo del personale scolastico include i seguenti compiti: - essere consapevoli dei problemi di sicurezza online connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili; - segnalare qualsiasi abuso, sospetto o problema ai responsabili della sicurezza online; - usare comportamenti sicuri, responsabili e professionali nell'uso della tecnologia.
Gli/le Alunni/e	Il ruolo degli alunni include i seguenti compiti: · essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti; · avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali; · comprendere l'importanza di adottare buone pratiche di sicurezza online (rapportate al grado di maturità e all'età degli studenti) quando si utilizzano le tecnologie digitali per non correre rischi; · adottare condotte rispettose degli altri anche quando si comunica in rete; · esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.
I Genitori	Il ruolo dei genitori degli alunni include i seguenti compiti: · Sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica; · Seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di internet; · Concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso

	non responsabile o pericoloso delle tecnologie digitali o di internet; · Fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e del telefonino in generale.

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

La E-Safety Policy sarà comunicata al personale, agli/alle alunni/e,alla comunità nei seguenti modi:

ALUNNI/E:

- Presentazione della E-Safety nelle classi quarte e quinte della scuola Primaria e nella scuola Secondaria di Primo grado;
- Affissione dell'elenco delle regole per la sicurezza online in tutte le aule e laboratori con accesso ad internet;
- Pubblicazione della versione integrale della E-Safety sul sito web dell'Istituto;
- Collaborazione tra scuola e famiglia sulla condivisione di regole comuni sulla sicurezza nell'uso delle TIC e di Internet;
- Formazione sull'argomento in occasione degli incontri scuola-famiglia, incontri collegiali e individuali.

PERSONALE SCOLASTICO:

- Comunicazione e condivisione del presente documento negli organi collegiali e successiva pubblicazione sul sito web dell'Istituto integrato con altro materiale informativo;
- Distribuzione di una copia dell'E-Safety Policy in ogni plesso dell'Istituto Comprensivo per la libera consultazione.

GENITORI:

- Comunicazione del presente documento e pubblicazione sul sito web dell'Istituto integrato con altro materiale informativo;
- Sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali;
- I docenti di classe forniranno ai genitori indirizzi sul web relativi a risorse utili per lo studio e a siti idonei ed educativi per gli alunni, sistemi di filtraggio e attività educative per il tempo libero.

1.4. Gestione delle infrazioni alla Policy.

1) Disciplina degli alunni

Le potenziali infrazioni in cui è possibile che gli/le alunni/e incorrano a scuola nell'utilizzo delle tecnologie digitali di internet di cui si dispone per la didattica, in relazione alla fascia di età considerate, sono prevedibilmente le seguenti:

- un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;

- l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;
- la condivisione di immagini intime o troppo spinte;
- la comunicazione incauta e senza permesso con sconosciuti;
- il collegamento a siti web non indicati dai docenti.

Gli interventi correttivi previsti per gli/le alunni/e sono rapportati all'età e al livello di sviluppo dell'alunno/a.
Infatti più gli/le alunni/e sono piccoli/e, più i comportamenti "da correggere" sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, che devono essere compresi e orientati proprio dagli educatori, nella prospettiva del raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno/a. Sono previsti pertanto da parte dei docenti provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento, quali:
- il richiamo verbale;
- il richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);
- il richiamo scritto con annotazione sul diario/libretto delle comunicazioni;
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente scolastico.

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli/delle alunni/e della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni.

2) Disciplina del personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet sono diverse e alcune possono determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli/delle alunni/e:
- un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- un trattamento dei dati personali, comuni e sensibili degli/delle alunni/e, non conforme ai principi della privacy o che non garantisca un' adeguata protezione degli stessi;
- una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- una carente istruzione preventiva degli/delle alunni/e sull'utilizzazione corretta e responsabile delle tecnologie digitali e di internet;
- una vigilanza elusa dagli/dalle alunni/e che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;

I docenti e il Dirigente scolastico devono controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informa-

tico della scuola, conservandone una copia per eventuali successive investigazioni. Tutto 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, civile e penale, a seconda del tipo o della gravità delle infrazioni commesse (si fa particolare riferimento ad eventi relativi a bullismo, cyberbullismo, violazione di privacy, diffamazione e maltrattamenti). Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

3) Disciplina dei genitori

In considerazione dell'età degli/delle alunni/e e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli/delle alunni/e a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico. Le situazioni familiari meno favorevoli sono:
- la convinzione che se il/la proprio/a figlio/a rimane a casa ad usare il computer è al sicuro e non combinerà guai;
- una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal/dalla proprio/a figlio/a;
- una piena autonomia concessa al/alla proprio/a figlio/a nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone;
- un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei;
- un utilizzo del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria indirizzi o contenuti non idonei.

I genitori degli/delle alunni/e possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei/delle loro figli/e se dovessero risultare pericolosi per sé 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 svolta ogni anno. Tale monitoraggio sarà curato dalla Dirigente Scolastica con la collaborazione dell'Animatore digitale, dalla Referente per le attività di prevenzione e contrasto del bullismo e cyber bullismo, dal team digitale e dai docenti delle classi, tramite questionari e conversazioni. L'aggiornamento della policy sarà curato dalla Dirigente Scolastica, dall'Animatore digitale, dalla Referente per le attività di prevenzione e contrasto del bullismo e cyber bullismo, dagli Organi Collegiali, a seconda degli aspetti considerati.

1.6. Integrazione della Policy con Regolamenti esistenti

La policy si integra con il REGOLAMENTO DI ISTITUTO quanto a norme comportamentali relative all'uso delle dotazioni tecnologiche della Scuola, della rete wifi e del traffico internet e dei Laboratori informatici.

2. FORMAZIONE E CURRICOLO

2.1. Curricolo sulle 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".

Il Curricolo della scuola del primo ciclo di istruzione sulle competenze digitali per gli/le alunni/e è trasversale alle discipline previste dalle Indicazioni Nazionali: la competenza digitale è ritenuta dall'Unione Europea competenza chiave, per la sua importanza e pervasività nel mondo d'oggi. L'approccio per discipline scelto dalle Indicazioni non consente di declinarla con le stesse modalità con cui si possono declinare le competenze chiave nelle quali trovano riferimento le discipline formalizzate. Si ritrovano abilità e conoscenze che fanno capo alla competenza digitale in tutte le discipline e tutte concorrono a costruirla. Competenza digitale significa padroneggiare certamente 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/e gli/le insegnanti e tutti gli insegnamenti sono coinvolti nella sua costruzione.

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

Il corpo docente ha partecipato e parteciperà a corsi di formazione e ad iniziative organizzate dall'istituzione o dalle scuole associate nella rete dell'Ambito di appartenenza. È inoltre disponibile ad aggiornarsi per mantenere al passo la propria formazione, in rapporto al rinnovo della dotazione multimediale.

Il percorso complesso della formazione specifica dei/delle docenti sull'utilizzo delle TIC nella didattica, non esauribile nell'arco di un anno scolastico, può pertanto prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva anche all'interno dell'istituto.

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

Anche il percorso della formazione specifica dei/delle docenti sull'utilizzo consapevole e sicuro di Internet, può prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i/le ragazzi/e.

Sarà predisposta una sezione nel sito dell'Istituto per la messa a disposizione e la condivisione di materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di internet. Qui sarà possibile trovare materiali informativi sulla sicurezza in internet per l'approfondimento personale e per le attività con gli/le studenti/esse ed eventuali contributi della Polizia di Stato, dell'Arma dei Carabinieri, di Telefono Azzurro, dal sito "Generazioni connesse", ecc.

2.4. Sensibilizzazione delle famiglie

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

particolare riferimento alla prevenzione del cyberbullismo. Sul sito scolastico e sulla relativa bacheca virtuale relativa a "Generazioni Connesse" saranno messi in condivisione materiali dedicati ad alunni/e e alle famiglie come guide in formato .pdf e video che possono fornire spunti di approfondimento e confronto.
La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento (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 a internet: filtri, antivirus e sulla navigazione.

- L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante;
- Internet non può essere usato per scopi vietati dalla legislazione vigente;
- L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet, dei social-media e delle chat;
- E' vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza.

Norme finali

Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

3.2. Gestione accessi (password, backup, ecc.)

L'accesso nei laboratori multimediali è consentito a tutto il personale docente.
I docenti registrano il proprio accesso, scrivendo su un registro la data e l'orario di utilizzo del laboratorio. Non in tutti i Plessi vi è un backup dei file elaborati, se non quello operato dai docenti interessati sui supporti rimovibili personali. Le postazioni del laboratorio funzionano come stazioni di lavoro e non come archivi.

3.3. E-mail

In ottemperanza a quanto richiesto dal MIUR e dal Ministero per la semplificazione e la Pubblica Amministrazione, in materia di digitalizzazione e informatizzazione della PA, e al fine ottimizzare il servizio scolastico ed assicurare modalità di rapporto corrette ed efficaci all'interno dell'Istituto, tutto il personale in servizio presso l'IC "Cervia2" è fornito di un indirizzo personale di posta elettronica ministeriale e un indirizzo di posta elettronica di G suite for Education.
Tutte le comunicazioni, gli avvisi, le convocazioni, le circolari interne ecc. sono inviate/i tramite e-mail alla casella di posta G Suite.
Tutte le comunicazioni, gli avvisi e le circolari divulgati tramite sito web o inviati per posta elettronica si intendono regolarmente notificati a tutto il personale.
Le circolari/avvisi segnalati come urgenti che comportano presa visione/adesione ad personam ed eventuale riscontro in Segreteria saranno trasmesse e divulgate anche con modalità diverse.
Si invita pertanto tutto il personale ad effettuare giornalmente l'accesso alla posta e consultare il sito web www.iccervia2.gov.it

3.4. Blog e sito web della scuola

La scuola attualmente ha un sito web. Tutti i contenuti del settore didattico sono pubblicati sotto la supervisione della Dirigente Scolastica, che valuta la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc..

3.5. Protezione dei dati personali

Il personale scolastico è "incaricato del trattamento" dei dati personali (degli/delle alunni/e, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Tutto il personale incaricato riceve poi istruzioni particolareggiate applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi. Viene inoltre fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli/delle alunni/e eccedenti i trattamenti istituzionali obbligatori.

4. STRUMENTAZIONE PERSONALE

4.1. Per gli/le studenti/esse: gestione degli strumenti personali - cellulari, tablet ecc.

Non è consentito alcun uso di strumenti elettronici personali e solo eccezionalmente quello del cellulare in caso di urgenza per comunicazioni tra gli/le alunni/e e le famiglie, su autorizzazione e con controllo dell'identità dell'interlocutore verificata dal docente.

4.2. Per i/le docenti: gestione degli strumenti personali - cellulari, tablet ecc.

Durante le ore delle lezioni non è consentito l'utilizzo del cellulare, mentre è consentito l'uso di altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili.
Durante il restante orario di servizio è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente mentre è permesso l'uso di altri dispositivi elettronici personali per attività funzionali all'insegnamento, ad integrazione di quelli scolastici disponibili.

4.3. Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc.

Durante l'orario di servizio al restante personale scolastico è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

a. Prevenzione

RISCHI	AZIONI
I rischi effettivi che si possono correre a scuola nell'utilizzo delle TIC da parte degli/delle alunni/e derivano da un uso non corretto del telefono cellulare personale o dello smartphone dei pc della scuola collegati alla rete. Il telefono cellulare o lo smartphone non sono richiesti dalla scuola perché non sono ritenuti indispensabili in ambito scolastico, ma vengono forniti dai genitori degli/delle alunni/e soprattutto per mantenere la comunicazione diretta con i/le figli/e anche fuori dal contesto scolastico. Eludendo la sorveglianza degli/delle insegnanti, attraverso i telefoni cellulari o gli smartphone, dotati di particolari applicazioni e di collegamento a internet, oltre che parlare e scrivere messaggi con i genitori, gli/le alunni/e potrebbero anche scaricare e spedire foto personali o intime, proprie o di altri, video con contenuti indecenti o violenti, accedere a internet e a siti non adatti ai minori, ascoltare musica e giocare con i videogiochi non consigliati ai minori, leggere la posta elettronica e comunicare o chattare con sconosciuti, inviare o ricevere messaggi molesti e minacciosi. Eludendo sempre la vigilanza degli/delle insegnanti, gli/le alunni/e potrebbero correre gli stessi rischi a scuola anche con l'utilizzo dei pc del laboratorio informatico e con un accesso non controllato a internet.	**Le azioni previste di prevenzione nell'utilizzo delle TIC sono le seguenti:** - Informare e formare i/le docenti, i genitori, il personale ATA, gli/le studenti/esse sui rischi che un uso non sicuro delle nuove tecnologie può favorire; - Fornire ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli/delle alunni/e eccedenti i trattamenti istituzionali obbligatori (es. liberatoria per la pubblicazione delle eventuali foto, immagini, testi e disegni relativi al proprio/a figlio/a); - Non consentire l'utilizzo del cellulare personale degli/delle alunni/e a scuola, in quanto per assolvere a ogni comunicazione urgente con i genitori o con chi ne fa le veci è sempre disponibile il telefono della scuola supervisionato dal personale addetto al centralino, che prima di passare la telefonata si accerta dell'identità dell'interlocutore; **Le azioni di contenimento degli incidenti previste sono le seguenti:** - Se la condotta incauta dell'alunno/a consiste nel fare circolare immagini imbarazzanti, di natura sessuale, su internet, è necessario rimuoverle; - Se l'alunno/a viene infastidito od offeso, suggerirgli di modificare i dettagli del proprio profilo sistemandolo su "privato", in modo tale che solo gli utenti autorizzati siano in grado di vederlo (MSN messengers, siti social network, Skype, etc.), o suggerirgli di bloccare o ignorare particolari mittenti, di cancellare il loro nominativo dalla lista degli amici e delle amiche con cui regolarmente chatta, di inserire il/la compagno/a o la persona che offende, per quanto riguarda l'e-mail, tra gli/le indesiderati/e; - Consigliare di cambiare il proprio indirizzo e-mail, di scaricare un'applicazione che blocchi chiamate e messaggi da numeri indesiderati o, se necessario, cambiare il numero di cellulare

	contattando l'operatore telefonico; - Far cancellare il materiale offensivo dal telefonino, facendo intervenire i genitori, e chiedere agli/alle studenti/esse di indicare a chi e dove lo hanno spedito per farlo fare anche gli altri, e conservare una copia di detto materiale se necessario per ulteriori indagini; - Contattare la polizia se si ritiene che il materiale offensivo sia illegale. In caso di foto e video pedopornografici, confiscare il telefonino o altri dispositivi ed evitare di eseguire download, produrne copie, condividerne link o postarne il contenuto, poiché ciò è reato per chiunque.

b. Rilevazione	
CHE COSA SEGNALARE	**COME SEGNALARE: QUALI STRUMENTI E A CHI E COME GESTIRE LE SEGNALAZIONI**
Gli/Le alunni/e possono mostrare segni di tristezza o di ansia o di risentimento nei confronti di compagni/e o di altri e riferire spontaneamente o su richiesta l'accaduto ai/alle docenti. I fatti riferiti possono essere accaduti anche al di fuori della scuola. Anche confrontandosi periodicamente con gli/le alunni/e sui rischi delle comunicazioni online, i/le minori/enni possono riferire di fatti o eventi personali o altrui che "allertano" l'insegnante. Una "prova" di quanto riferito può essere presente nella memoria degli strumenti tecnologici utilizzati, può essere mostrata spontaneamente dall'alunno/a, può essere presentata da un reclamo dei genitori, può essere notata dall'insegnante che si accorge dell'infrazione in corso. Mentre il/la docente è autorizzato/a a controllare le strumentazioni della scuola, per controllare l'uso del telefono cellulare di un alunno/a si rivolge al genitore. I contenuti "pericolosi" comunicati/ricevuti a/da altri/e, messi/scaricati in rete, ovvero le tracce che possono	Per il telefono cellulare ci si può assicurare che l'alunno/a vittima salvi nel suo telefono ogni messaggio, voce/testo/immagine, conservando così il numero del mittente. Gli insegnanti possono provvedere ugualmente a conservare le prove della condotta incauta, scorretta o dell'abuso rilevate sui pc della scuola: soprattutto la data e l'ora, il contenuto dei messaggi e, se possibile, l'ID del mittente (es. username, mail, numero di telefono cellulare) o l'indirizzo web del profilo ed il suo contenuto. Qualora ci si dovesse accorgere che l'alunno/a, usando il computer, si sta servendo di un servizio di messaggeria istantanea, programma che permette di chattare in linea tramite testo, l'insegnante può copiare, incollare e stampare la conversazione. Per gli eventuali collegamenti non autorizzati a siti social network, video-hosting sites e altri website, l'insegnante può conservare il link, stampare la pagina o salvare la schermata su documento word. Per le e-mail si può stampare l'e-mail o conservare l'intero messaggio, compresa l'intestazione del mittente. Conservare la prova è utile per far conoscere l'accaduto in base alla gravità ai genitori degli/delle alunni/e, alla Dirigente scolastica e per le condotte criminose alla polizia. Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno/a, quantunque riferite a fatti accaduti al di fuori del contesto scolastico, le notizie raccolte sono comunque comunicate ai genitori e per fatti rilevanti anche alla Dirigente scolastica; per quelle criminose, anche

comprovare l'utilizzo incauto, scorretto o criminoso degli strumenti digitali utilizzabili anche a scuola attualmente dai minori e dalle minorenni (l'eventuale telefonino/smartphone personale e il pc collegato a internet) per gli/le alunni/e possono essere i seguenti: - Contenuti afferenti alla privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici o amiche, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.); - Contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.); - Contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.	alla polizia. In particolare la segnalazione viene fatta a entrambe le famiglie, se oltre alla vittima anche l'autore/autrice della condotta negativa è un/una altro/a alunno/a. Per le segnalazioni di fatti rilevati sono previsti i seguenti strumenti che i/le docenti possono utilizzare sulla base della gravità dell'accaduto: ▪ Annotazione del comportamento sul registro e comunicazione scritta ai genitori, che la devono restituire vistata; ▪ Convocazione scritta e colloquio con i genitori degli/delle alunni/e, da parte dei/delle docenti; ▪ Relazione scritta alla Dirigente scolastica. In base all'urgenza le comunicazioni formali possono essere precedute da quelle informali, effettuate per le vie brevi. Inoltre per i reati meno gravi la legge rimette ai genitori degli/delle alunni/e la scelta di richiedere la punizione del colpevole, attraverso la querela. Per i reati più gravi (es. pedopornografia) gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti). In particolare per i fatti criminosi, ai fini della denuncia, la relazione deve essere redatta nel modo più accurato possibile, indicando i seguenti elementi: il fatto, il giorno dell'acquisizione del fatto nonché le fonti di prova già note e per quanto possibile, le generalità, il domicilio e quant'altro di utile a identificare la persona alla quale il reato è attribuito, la persona offesa, e tutti coloro che sono in grado di riferire circostanze rilevanti per la ricostruzione del fatto.

c. Gestione dei casi

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

Gestione dei casi di "immaturità"

Può sembrare naturale all'alunno/a fornire i propri dati sui siti allestiti in modo tale da attrarre l'attenzione dei/delle bambini/e, con giochi e animazioni, personaggi simpatici e divertenti, che richiedono una procedura di registrazione.

Curiosità, manifestazioni di reciproco interesse tra pari, idee e fantasie sulla sessualità sono espressione da una parte del progressivo sviluppo socio-affettivo dell'alunno/a e dall'altra dei molteplici messaggi espliciti che gli/le giungono quotidianamente attraverso i media (televisione, DVD, internet, giornali e riviste), i discorsi degli/delle altri/e bambini/e o degli adulti.

I comportamenti cosiddetti "quasi aggressivi", che spesso si verificano tra coetanei, le interazioni

animate o i contrasti verbali, o la presa in giro "per gioco", effettuata anche in rete, mettono alla prova la relazione con i/le compagni/e, la supremazia o la parità tra i soggetti implicati e l'alternanza e sperimentazione dei diversi ruoli. Il gruppo dei pari rappresenta anche il momento di conquista dell'autonomia dall'adulto e pertanto luogo di "complicità" e di piccole "trasgressioni", di scambi "confidenziali" condivisi fra gli amici nella rete o con il cellulare.
Detti comportamenti, che finiscono per arrivare all'attenzione degli adulti, sono controllati e contenuti dai/dalle docenti attraverso i normali interventi educativi, di richiamo al rispetto delle regole di convivenza civile e democratica, di rispetto degli altri, per evitare che possano degenerare, diventare pericolosi per sé o offensivi e minacciosi per gli/le altri/altre.

Gestione dei casi di "prepotenza" o "prevaricazione"

I comportamenti definibili come "**Bullismo**" possono esprimersi nelle forme più varie e non sono tratteggiabili a priori; se non contestualizzandoli. Le caratteristiche che aiutano a individuarli e a distinguerli dallo scherzo, dalle intemperanze caratteriali, dai diverbi usuali fra i ragazzi e le ragazze sono la costanza nel tempo e la ripetitività, l'asimmetria (disuguaglianza di forza e di potere), il disagio della/e vittima/e.
Il bullismo si esplica infatti con comportamenti e atteggiamenti costanti e ripetitivi di arroganza, prepotenza, prevaricazione, disprezzo, dileggio, emarginazione, esclusione ai danni di una o più persone, agiti da un solo soggetto, ma in genere da un gruppo.
Nel caso particolare del **Cyberbullismo** le molestie sono attuate attraverso strumenti tecnologici:

- invio di sms, messaggi in chat, e-mail offensive o di minaccia;
- diffusione di messaggi offensivi ai danni della vittima, attraverso la divulgazione di sms o e-mail nelle mailing-list o nelle chat-line;
- pubblicazione nel cyberspazio di foto o filmati che ritraggono prepotenze o in cui la vittima viene denigrata.

Rientrano nel Cyberbullismo:

- *Flaming*: Litigi on line nei quali si fa uso di un linguaggio violento e volgare.
- *Harassment*: molestie attuate attraverso l'invio ripetuto di linguaggi offensivi.
- *Cyberstalking*: invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la propria incolumità.
- *Denigrazione*: pubblicazione all'interno di comunità virtuali , quali newsgroup, blog, forum di discussione, messaggistica immediata, siti internet,… di pettegolezzi e commenti crudeli, calunniosi e denigratori.
- *Outing estorto*: registrazione delle confidenze – raccolte all'interno di un ambiente privato- creando un clima di fiducia e poi inserite integralmente in un blog pubblico.
- *Impersonificazione*: insinuazione all'interno dell'account di un'altra persona con l'obiettivo di inviare dal medesimo messaggi ingiuriosi che screditino la vittima.
- *Esclusione*: estromissione intenzionale dall'attività on line.
- *Sexting*: invio di messaggi via smartphone ed Internet, corredati da immagini a sfondo sessuale.

Il bullismo in particolare può originarsi anche dall'esasperazione di conflitti presenti nel contesto scolastico. Il conflitto, presente in ogni normale intenzione, è da considerarsi come un campanello d'allarme e può degenerare in forme patologiche quando non lo si riconosce e gestisce in un'ottica evolutiva dei rapporti, di negoziazione e risoluzione. Se non gestito positivamente, infatti, il conflitto rischia di mutarsi e provocare effetti distruttivi sulle relazioni (prevaricazione e sofferenza) e sull'ambiente (alterazione del clima del gruppo-classe).

In considerazione dell'età degli/delle alunni/e considerati/e possono prefigurarsi alcune forme di interazioni che possono evolvere verso tale fenomeno. Per prevenire e affrontare il bullismo dunque i/le docenti non solo identificano vittime e prepotenti in divenire, ma tutti insieme affrontano e intervengono sul gruppo-classe, coinvolgendo i genitori degli/delle allievi/e.
L'elemento fondamentale per una buona riuscita dell'intervento educativo è infatti la corretta, compiuta e convinta ristrutturazione dell'ambiente sociale in cui tale fenomeno si verifica, e in particolare delle relazioni nel contesto della classe. Gli atteggiamenti degli/delle alunni/e, così come quelli dei loro genitori, possono giocare un molto significativo nel ridurre la dimensione del fenomeno.
Gli interventi mirati sul gruppo classe sono gestiti in collaborazione dal team dei/delle docenti della classe e d'intesa con le famiglie, ad esempio, con percorsi di mediazione volta alla gestione positiva del conflitto, con gruppi di discussione (circle time), con rappresentazioni e attività di role-play sull'argomento del bullismo, con le strategie del problem solving.
Vengono intrapresi anche i percorsi individualizzati di sostegno alle vittime, volti a incrementarne l'autostima e l'assertività e a potenziare le risorse di interazione sociale, mentre i prevaricatori sono destinatari di interventi mirati a smuoverne le competenze empatiche e a favorire una loro condivisione delle norme morali.
Anche in relazione alle manifestazioni socio-affettive fra pari, al linguaggio sessualizzato o "volgare", al fine di evitare prevaricazioni e imbarazzo o disagio, i/le docenti intervengono per favorire nei/nelle bambini/e un buon rapporto con il proprio corpo e per far percepire meglio eventuali violazioni dei limiti di prossimità o di "confidenza" ed imparare ad opporvisi, per far acquisire fiducia nelle proprie sensazioni e nel proprio intuito e determinazione nel rifiutare i contatti anche "a distanza" sgradevoli o "strani", per rendere consapevoli gli alunni e le alunne del diritto al rispetto dei propri limiti e di quelli altrui, per far capire ai ragazzi e alle ragazze che l'interazione online deve sottostare a delle regole di buon comportamento, né più né meno della comunicazione a viso aperto, quale quella della vita reale.
Inoltre, la scuola, qualora rilevi una situazione psico-socio-educativa particolarmente problematica, convoca i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi. Promuove e supporta la richiesta delle famiglie rivolta ai Servizi Sociali dell'Ente Locale per la fruizione di servizi socio-educativi comunali e alla ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare).

A chi segnalare:
L'attuazione del programma di intervento si basa prevalentemente sull'impiego delle risorse umane già presenti e disponibili: insegnanti e altro personale scolastico, alunni/e e genitori. Non serve, se non in casi particolarmente gravi, l'opera di psicologi, assistenti sociali, o altri specialisti a cui orientare la famiglia.
L'elemento fondamentale per una buona riuscita del programma è infatti la corretta ristrutturazione del contesto relazionale degli/delle alunni/e.

Gestione degli "abusi sessuali"

"In generale si parla di abuso sessuale sui bambini o sulle bambine quando un/una bambino/a viene coinvolto/a in un atto sessuale. Ciò è caratterizzato dal fatto che il/la bambino/a non comprende del tutto tale atto, non è informato e quindi non è in grado di acconsentire, oppure sulla base del suo livello di sviluppo non è ancora pronto per tale atto e non può dare il proprio consenso".
Lo spettro delle forme di abuso e di violenza è diventato ancora più ampio e subdolo in seguito

alle possibilità offerte dai nuovi mezzi di comunicazione come internet, il cellulare o altri dispositivi tecnologici, e il loro utilizzo sempre più diffuso non fa che acuire il problema. Internet, infatti, permette di scaricare o vendere immagini o filmati di pornografia infantile.
Succede sempre più frequentemente che un adulto prenda contatto con dei/delle bambini/e nei forum o nelle chat su internet, e che li metta di fronte a domande o messaggi sessuali o addirittura a immagini pornografiche. A volte l'adulto induce i/le bambini/e a spogliarsi davanti alla webcam oppure a inviare una fotografia che li ritrae nudi tramite internet o sul cellulare, per poi ricattarli e costringerli a non rivelare gli abusi. Spesso l'adulto finge di essere minorenne.
La denuncia all'autorità giudiziaria o agli organi di Polizia, da parte degli/delle insegnanti o della Dirigente Scolastica, 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. I versanti su cui si articola l'intervento possono essere essenzialmente tre: medico, socio-psicologico e giudiziario.
Il compito della scuola non è comunque solo quello di "segnalare", **ma** più ampio ed importante, **soprattutto nella prevenzione dell'abuso**, nonché nella ripresa della piccola vittima, in quanto ha al suo interno fattori relazionali ed educativi che possono aiutare il/la bambino/a a riprendere una crescita serena.
A tal fine la scuola lavora insieme alle altre figure professionali e alle famiglie, scambiando informazioni e condividendo progetti e prassi operative, favorendo le occasioni di confronto e di dialogo.

A chi segnalare:
In particolare nel caso in cui ci si dovesse imbattere in materiale pedopornografico (cioè contenuti foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali), è necessario, innanzitutto, evitare di eseguire download, produrne copie, condividerne link o postarne il contenuto. Ciò è reato per chiunque. Nel venire a conoscenza di materiali di questo tipo è importante contribuire alla loro eliminazione: basta inserire le informazioni richieste sugli appositi moduli online, disponibili ai siti www.stop-it.it e http://www.azzurro.it/it/clicca-e-segnala" ovvero collegandosi al sito della **polizia postale** https://www.commissariatodips.it, ove è possibile sia segnalare che denunciare. In alternativa è possibile recarsi nella sede più vicina della polizia giudiziaria. Ciò consente di operare con la massima tempestività.
Non operare in modo isolato, ma confrontarsi con i colleghi di classe e la Dirigente Scolastica.

6. ANNESSI **(a cura dell'Istituto)**

6.1. Procedure operative per la gestione delle infrazioni alla Policy.

a. MODULO DI RICHIESTA PER L'ACCESSO AD INTERNET NELLA RETE DI ISTITUTO E PER L'UTILIZZO DEI DISPOSITIVI ELETTRONICI

b. MODULO DI RICHIESTA DI CREDENZIALI DI AUTENTICAZIONE/DI ACCESSO AD INTERNET NELLA RETE DI ISTITUTO E DI UTILIZZO DEI DISPOSITIVI ELETTRONICI

6.2. Procedure operative per la protezione dei dati personali.

a. DICHIARAZIONE LIBERATORIA DEI GENITORI/TUTORI PER LA PUBBLICAZIONE DI ELABORATI, NOMI, VOCI, IMMAGINI, MATERIALE AUDIOVISIVO

Codice MIUR RAIC829007 - C.F. 92082630390
Via Caduti per la Libertà, 16 - 48015 CERVIA (RA) - tel.0544/71955 fax 0544/72246
E mail: raic829007@istruzione.it - Pec: raic829007@pec.istruzione.it
web: www.iccervia2.gov.it

Procedure operative per la gestione delle infrazioni alla Policy

MODULO DI RICHIESTA PER L'ACCESSO AD INTERNET NELLA RETE DI ISTITUTO E PER L'UTILIZZO DEI DISPOSITIVI ELETTRONICI

Al Dirigente Scolastico

Istituto Comprensivo "Cervia2"

Il/La sottoscritto/a _____, nato/a a_____ (___),

il _____, residente a _____

in via _____, n. _____CAP _____

e-mail _____

in qualità di genitore dell'alunno/a_____,

iscritto/a alla classe ……sez. ……. dell'Istituto Comprensivo "Cervia2"

- **Dichiara** di essere consapevole delle implicazioni di responsabilità personale derivanti dall'accesso alla rete internet e dell'uso del cellulare e dagli eventuali abusi. In particolare si impegna a che il/la figlio/a:

- non scarichi/duplichi/distribuisca software o altri contenuti protetti da diritto d'autore;

- non acceda a siti o risorse dal contenuto illegale o non consono alle regole di comportamento dettate dal carattere istituzionale ed educativo della scuola (ad esempio, siti con contenuto violento, pedo-pornografico, razzista, ecc.);

- non diffonda virus o altri software malevoli all'interno della rete e a dare immediato avviso all'Amministrazione della Rete di comportamenti anomali o di infezioni riconosciute;

- non utilizzi il cellulare o altri dispositivi elettronici personali a scuola;

- partecipi con impegno agli interventi educativi della scuola sulle modalità di utilizzo sicuro e consentito dei dispositivi elettronici e di internet.

Data _____ Firma leggibile _____

Codice MIUR RAIC829007 - C.F. 92082630390
Via Caduti per la Libertà, 16 - 48015 CERVIA (RA) - tel.0544/71955 fax 0544/72246
E mail: raic829007@istruzione.it - Pec: raic829007@pec.istruzione.it
web: www.iccervia2.gov.it

Procedure operative per la gestione delle infrazioni alla Policy

MODULO DI RICHIESTA DI CREDENZIALI DI AUTENTICAZIONE/DI ACCESSO AD INTERNET NELLA RETE DI ISTITUTO E DI UTILIZZO DEI DISPOSITIVI ELETTRONICI

Al Dirigente Scolastico

Istituto Comprensivo "Cervia2"

Il/La sottoscritto/a _____, nato/a a_____ (___),

il _____, residente a _____

in via _____, n. _____CAP _____

e-mail _____

in qualità di docente/personale ATA (cancellare la voce che non interessa) in servizio presso l'I C "Cervia2" chiede il rilascio delle credenziali di autenticazione /l'accesso ad Internet nella rete di Istituto.

Dichiara:

- di aver letto e compreso il documento di "Policy E-Safety", di utilizzo accettabile della rete internet, pubblicato sul sito della Scuola;
- di essere consapevole delle implicazioni di responsabilità personale derivanti dall'accesso alla rete internet e dagli eventuali abusi. In particolare si impegna a:
- non scaricare/duplicare/distribuire software o altri contenuti protetti da diritto d' autore;
- non accedere a siti o risorse dal contenuto illegale o non consono alle regole di comportamento dettate dal carattere istituzionale ed educativo della scuola (ad esempio, siti con contenuto violento, pedo-pornografico, razzista, etc…);
- non collegarsi ad internet a scopi commerciali o di profitto personale e per attività illegali;
- non diffondere virus o altri software malevoli all'interno della rete e a dare immediato avviso all'Amministrazione della Rete di comportamenti anomali o di infezioni riconosciute;

- conservare le credenziali di accesso alla rete in modo scrupoloso, non comunicandole ad altre persone. E' consapevole che l'accesso attraverso l'autenticazione trasferisce direttamente la responsabilità degli atti commessi durante la navigazione all'intestatario delle credenziali stesse.

Dichiara di essere consapevole che:

- l'autorizzazione all'uso della rete di Istituto potrà venire revocata (cancellazione dell'utente) in qualsiasi momento per cause tecniche o per motivazioni legate all'uso improprio o alla violazione delle norme di comportamento;
- l'utilizzo dei dispositivi elettronici e della rete della scuola deve essere utilizzata per attività di servizio o funzionali alle stesse;
- l'utilizzo della rete per l'assunzione di impegni o responsabilità per conto della scuola deve essere autorizzata dalla dirigente scolastica, legale rappresentante dell'istituzione nonché legittimo titolare dell'utenza;
- l'utilizzo del cellulare e di altri dispositivi elettronici personali a scuola deve avvenire nei limiti consentiti dalla legge e dai regolamenti dell'istituzione scolastica, in situazioni di necessità ed urgenza opera ragioni di servizio;
- ci si deve rivolgere per la necessaria assistenza alla connessione o al funzionamento dei dispositivi contattando il referente del laboratorio di informatica (o l'Animatore digitale) o gli uffici di segreteria, evitando tentativi incerti di ripristino o di modificazione delle impostazioni.

Data _____ Firma leggibile _____

Codice MIUR RAIC829007 - C.F. 92082630390
Via Caduti per la Libertà, 16 - 48015 CERVIA (RA) - tel.0544/71955 fax 0544/72246
E mail: raic829007@istruzione.it - Pec: raic829007@pec.istruzione.it
web: www.iccervia2.gov.it

Procedure operative per la protezione dei dati personali.

DICHIARAZIONE LIBERATORIA DEI GENITORI/TUTORI PER LA PUBBLICAZIONE DI ELABORATI, NOMI, VOCI, IMMAGINI, MATERIALE AUDIOVISIVO

Al Dirigente Scolastico

Istituto Comprensivo "Cervia2"

Io sottoscritto_____, nato a _____(____),

il _____, residente a _____ (_____),

indirizzo: _____;

Io sottoscritta_____, nata a _____(____),

il _____, residente a _____ (_____),

indirizzo: _____;

genitori dell'alunno/a _____

frequentante la scuola_____classe _____ sez. _____

AUTORIZZIAMO l'Istituto Comprensivo "Cervia2" nella persona del Dirigente Scolastico a realizzare fotografie, video o altri materiali audiovisivi contenenti l'immagine, il nome e la voce del proprio figlio/a, all'interno di attività educative e didattiche, per scopi documentativi, formativi ed informativi.

Il Dirigente Scolastico dell'Istituto Comprensivo "Cervia2" assicura che le immagini e le riprese audio-video realizzate nella scuola, nonché gli elaborati prodotti dagli studenti durante le attività scolastiche, potranno essere utilizzati esclusivamente per documentare e divulgare le attività della scuola tramite il sito internet di Istituto, pubblicazioni, mostre, corsi di formazione, seminari, convegni ed altre iniziative promosse dall'istituto anche in collaborazione con altri enti pubblici. La presente autorizzazione non consente l'uso dell'immagine in contesti che pregiudichino la dignità personale e decoro del minore e comunque per uso e/o fini diversi da quelli sopra descritti.

La presente autorizzazione è valida per tutti gli anni di permanenza dell'alunno/a nella suddetta scuola.

Luogo e data_____/____/_____

In fede…….. In fede……..

(firme leggibili di entrambi i genitori)

Allegati: fotocopie dei documenti d' identità

6.3. **Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni**

CYBERBULLISMO: alcuni campanelli di allarme

Gli atti di bullismo avvengono prevalentemente entro o nei dintorni del contesto scolastico, tuttavia in misura crescente le prepotenze vengono riportate nel contesto virtuale di internet. In queste situazioni si parla di cyberbullismo che si manifesta attraverso:

- invio di sms, mms, e-mail offensivi/e o di minaccia;
- diffusione di messaggi offensivi ai danni della vittima, attraverso la divulgazione di sms o e-mail nelle mailing-list o nelle chat-line;
- pubblicazione nel cyberspazio di foto o filmati che ritraggono prepotenze o in cui la vittima viene denigrate.

La rilevazione diretta degli indicatori da parte degli/delle insegnanti o indiretta, sulla base di quanto riferito dagli/dalle alunni/e o dai genitori, deve affinarsi con l'osservazione delle relazioni interpersonali e delle possibili dinamiche conflittuali sottostanti presenti nel contesto classe, al fine di verificare l'entità e la natura del fenomeno e dare avvio al programma di intervento.

6.4. **Procedure operative per la gestione dei casi**

LINEE GUIDA PER ALUNNI/E

- Non comunicare mai a nessuno la tua password e periodicamente cambiala, usando numeri, lettere caratteri speciali;
- Mantieni segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della tua scuola;
- Non inviare a nessuno fotografie tue o di tuoi amici e tue amiche;
- Prima di inviare o pubblicare su un BLOG la fotografia di qualcuno/a, chiedi sempre il permesso;
- Chiedi sempre al/alla tuo/a insegnante a scuola o ai tuoi genitori a casa il permesso di scaricare documenti da Internet;
- Chiedi sempre il permesso prima di iscriverti a qualche concorso o prima di riferire l'indirizzo della tua scuola;
- Quando sei connessi alla rete RISPETTA SEMPRE GLI ALTRI, ciò che per te è un gioco può rivelarsi offensivo per qualcun altro;
- Non rispondere alle offese ed agli insulti;
- Blocca i Bulli: molti Blog e siti social network ti permettono di segnalare i cyberbulli;
- Conserva le comunicazioni offensive, ti potrebbero essere utili per dimostrare quanto ti è accaduto;
- Rifletti prima di inviare: ricordati che tutto ciò che invii su internet diviene pubblico e rimane per SEMPRE;
- Riferisci al/alla tuo/a insegnante o ai tuoi genitori se qualcuno ti invia immagini che ti infastidiscono e non rispondere; riferisci anche al/alla tuo/a insegnante o ai tuoi genitori se ti capita di trovare immagini di questo tipo su Internet;
- Se qualcuno su Internet ti chiede un incontro di persona, riferiscilo al/alla tuo/a insegnante o ai tuoi genitori;
- Ricordati che le persone che incontri nella Rete sono degli estranei e non sempre sono quello che dicono di essere;

- Non è consigliabile inviare e-mail personali, perciò rivolgiti sempre al/alla tuo/a insegnante prima di inviare messaggi di classe o ai tuoi genitori prima di inviare messaggi da casa;
- Non scaricare (download) o copiare materiale da Internet senza il permesso del/della tuo/a insegnante o dei tuoi genitori;
- Non caricare (upload) materiale video o fotografico nei siti web dedicati senza il permesso del/della tuo/a insegnante o dei tuoi genitori.

LINEE GUIDA PER INSEGNANTI

- Evitate di lasciare le e-mail o file personali sui computer o sul server della scuola, lo spazio è limitato e di uso comune;
- Salvate sempre i vostri lavori (file) in cartelle personali e/o di classe e non sul desktop o nella cartella del programma in uso. Sarà cura di chi mantiene il corretto funzionamento delle macchine cancellare file di lavoro sparsi per la macchina e al di fuori delle cartelle personali;
- Discutete con gli alunni e con le alunne della Policy E-Safety della scuola, di utilizzo consentito della rete, e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'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 chiudere la connessione (e di spegnere il computer) alla fine della sessione di lavoro su Internet e disabilitare la navigazione su Internet del laboratorio (qualora sia stata attivata);
- Ricordate agli alunni e alle alunne che la violazione consapevole della Policy E-Safety della scuola, di utilizzo consentito della rete, comporta sanzioni di diverso tipo;
- Adottate provvedimenti "disciplinari", proporzionati all'età e alla gravità del comportamento;
- Adottate interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi, di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni e delle alunne della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni;
- Nelle situazioni psico-socio-educative particolarmente problematiche, convocate i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi (Servizi Sociali per la fruizione di servizi socio-educativi comunali, ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare);
- Chiedete/suggerite di cancellare il materiale offensivo, bloccare o ignorare particolari mittenti, uscire da gruppi non idonei, cambiare indirizzo e-mail, ecc...;
- Segnalate la presenza di materiale pedopornografico (senza scaricarlo o riprodurlo) alla Polizia Postale o al Telefono Azzurro;
- In caso di abuso sessuale rilevato anche attraverso i nuovi mezzi di comunicazione come internet o il cellulare, confrontatevi con i/le colleghi/e di classe e la Dirigente Scolastica, denunciate all'autorità giudiziaria o agli organi di Polizia.

CONSIGLI AI GENITORI PER UN USO RESPONSABILE DI INTERNET A CASA

Consigli generali

- Posizionate il computer in salone o in una stanza accessibile a tutta la famiglia;
- Evitate di lasciare le e-mail o file personali sui computer di uso comune;
- Concordate con vostro figlio/a le regole: quando si può usare internet e per quanto tempo;

- Inserite nel computer i filtri di protezione: prevenite lo spam, i pop-up pubblicitari, l'accesso a siti pornografici;
- Aumentate il filtro del "parental controll" attraverso la sezione sicurezza in internet dal pannello di controllo;
- Attivate il firewall (protezione contro malware) e antivirus;
- Mostratevi coinvolti: chiedete a vostro/a figlio/a di mostrarvi come funziona internet e come viene usato per scaricare e caricare compiti, lezioni, materiali didattici e per comunicare con l'insegnante;
- Incoraggiate le attività online di alta qualità: ricercare informazioni scientifiche, ricercare nuovi amici/amiche nel mondo;
- Partecipa alle esperienze online: naviga insieme a tuo/a figlio/a, incontra amici online, discuti gli eventuali problemi che si presentano;
- Comunicate elettronicamente con vostro/a figlio/a: inviate, frequentemente, e-mail, Instant Message;
- Spiegate a vostro/a figlio/a che la password per accedere ad alcune piattaforme è strettamente personale e non deve essere mai fornita ai compagni o ad altre persone;
- Stabilite ciò che ritenete inaccettabile (razzismo, violenza, linguaggio volgare, pornografia);
- Discutete sul tema dello scaricare file e della possibilità di ricevere file con virus;
- Raccomandate di non scaricare file da siti sconosciuti;
- Incoraggiate vostro/a figlio/a a dirvi se vedono immagini particolari o se ricevono e-mail indesiderate;
- Discutete nei dettagli le conseguenze che potranno esserci se vostro/a figlio/a visita deliberatamente siti non adatti, ma non rimproveratelo se compie azioni involontarie;
- Spiegate a vostro/a figlio/a che le password, i codici pin, i numeri di carta di credito e i numeri di telefono e i dettagli degli indirizzi e-mail sono privati e non devono essere dati ad alcuno;
- Spiegate a vostro/a figlio/a che non tutti in Internet sono chi realmente dichiarano di essere; di conseguenza i vostri ragazzi e le vostre ragazze non dovrebbero mai accordarsi per appuntamenti senza consultarvi prima;
- Il modo migliore per proteggere vostro/a figlio/a è usare Internet con loro, discutere e riconoscere insieme i rischi potenziali.

CONSIGLI IN BASE ALL'ETÀ

Se tuo/a figlio/a ha meno di 8 anni

- Seleziona con molta attenzione i siti "sicuri": ricordati che i gestori dei siti, per trarre il massimo guadagno, permettono agli inserzionisti di pubblicizzare i propri prodotti;
- Comunica a tuo/a figlio/a tre semplici regole:
  - non dare il tuo vero nome, indirizzo e numero di telefono. Usa sempre il tuo "computer username" o nickname;
  - se compare sullo schermo qualche messaggio o banner, chiudilo: insegna a tuo/a figlio/a come si fa;
  - naviga esclusivamente sui siti autorizzati dai genitori: se vuoi andare su un nuovo sito, dobbiamo andarci INSIEME (molti siti richiedono la registrazione. Insegna a tuo/a figlio/a come registrarsi senza rivelare informazioni personali).

Se tuo/a figlio/a ha tra gli 8 anni e i 10 anni

Progressivamente diminuisci la supervisione: dagli otto ai dieci anni permetti a tuo/a figlio/a di

navigare da solo nei siti autorizzati, sottolineando che deve consultarti prima di esplorarne dei nuovi. Verifica periodicamente i contenuti dei siti "sicuri". Discuti con tuo/a figlio/a i rischi che possono presentarsi durante la navigazione online. Controlla, dalla cronologia il menu navigazione, se tuo/a figlio/a ha consultato siti non autorizzati per i quali non ti ha chiesto il permesso. Supervisiona l'e-mail di tuo/a figlio/a dopo averlo reso consapevole del fatto che hai pieno accesso alle sue comunicazioni. Se tuo/a figlio/a vuole usare Instant Messanger (IM – Messaggistica istantanea) verifica che i suoi contatti siano limitati agli amici e alle amiche conosciuti/e. Specifica che non può inserire nuovi contatti senza averti prima consultato. Comunicagli che è assolutamente vietato cliccare su un link, contenuto in una e-mail, su un pop-up pubblicitario o su un banner (ricordati, infatti, che potrebbero presentarsi immagini pornografiche o che potrebbe avviarsi il download di "malware"). Incoraggia l'uso di internet per svolgere ricerche scolastiche. Definisci il tempo massimo di connessione ed incoraggia le attività con il mondo reale.

Se tuo/a figlio/a ha tra gli 11 anni e i 13 anni

Tuo/a figlio/a è diventato grande e potrebbe dirti che il/la suo/a migliore amico/a ha la possibilità di navigare tutti i giorni a tutte le ore …. Che fare? Crea una partnership con i genitori dei/delle migliori amici/amiche di tuo/a figlio/a in modo da concordare con loro le regole: tempi di connessione, fasce orarie, siti autorizzati, modalità di utilizzo di IM. Aiuta tuo/a figlio/a a creare una rete online sicura: siti controllati ed amici e amiche conosciuti.

Se tuo/a figlio/a ha oltre 13 anni

Verifica i profili di tuo/a figlio/a e dei/delle suoi amici/amiche, nei siti cerca persona, informandolo dei tuoi periodici controlli. Ricordati che in questa fascia di età aumentano le ricerche di materiale sessuale ed i rischi di seduzioni sessuali online da parte di cyberpredatori adulti: condividi con tuo/a figlio/a le procedure per navigare in sicurezza ed evitare on-line ed off-line brutti incontri. Confrontati con tuo/a figlio/a su tutti questi rischi e se protesta per il controllo, ribadisci che è un dovere del genitore supervisionare e monitorare l'uso di internet. Stringi un accordo: se tuo/a figlio/a dimostra di avere compreso i rischi e di sapere e volere usare internet in modo sicuro, diminuisci la supervisione. Il computer deve rimanere in salone o in una stanza accessibile a tutta la famiglia e non nella camera di tuo/a figlio/a ALMENO fino ai 16 anni.

7. PROTOCOLLI SIGLATI CON LE FORZE DELL'ORDINE E I SERVIZI DEL TERRITORIO PER LA GESTIONE CONDIVISA DEI CASI.

Non vi sono protocolli siglati ma ricorrenti forme di collaborazione nella prevenzione e contrasto del bullismo e del cyberbullismo da parte dell'Ente Locale e del Comando dei Carabinieri.

Versione	1.0
Data	05 marzo 2018
Approvato dal Dirigente Scolastico	
Approvato dal Collegio Docenti	
Approvato dal Consiglio di Istituto	
Prossima data di revisione	

IL DIRIGENTE SCOLASTICO
Dott.ssa Mariapia Metallo

[Firma autografa sostituita a mezzo stampa ai sensi dell'art.3, comma 2 del D.Lgs. 39/1993]