

i.c. CASALGRANDE



C.F.: 80015350350 - Cod. mec.: REIC833009

ISTITUTO COMPRENSIVO DI CASALGRANDE

Viale Gramsci, 21 – 42013 Casalgrande (RE) - reic833009@pec.istruzione.it
0522-846178/846242 info@iccasalgrande.edu.it www.iccasalgrande.edu.it



FONDI STRUTTURALI EUROPEI
pon
2014-2020
PER LA SCUOLA - COMPETENZE E AMBIENTI PER L'APPRENDIMENTO (FSE-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



Erasmus+

Policy di E-safety Politica per l'Uso Accettabile dei dispositivi e della Rete della Scuola

Approvato dal Consiglio di Istituto del 16/04/2019

Indice

Introduzione

- 1. Tecnologie, metodologie e internet nella scuola di oggi.**
- 2. Rischi e opportunità della Rete**
- 3. Ruoli e Responsabilità**
- 4. Gli spazi fisici e virtuali disponibili della scuola**
- 5. Strategie adottate per garantire la sicurezza delle TIC e pericoli della Rete**
- 6. Norme comportamentali dell'utente**
- 7. Documentazioni, Regolamenti, gestione dei casi**

Introduzione

Scopo del presente documento è quello di informare l'utenza delle procedure attivate dall'Istituto per un uso corretto e responsabile delle apparecchiature informatiche collegate alla Rete scolastica, nel rispetto della normativa vigente.

In particolare l'intento della scuola è quello di:

- attivare misure di prevenzione, rilevazione e gestione delle problematiche connesse ad un uso consapevole delle TIC;
- stabilire norme comportamentali e procedure per un utilizzo delle TIC in ambiente scolastico;
- assistere, salvaguardare e proteggere tutti gli utenti;
- formare e promuovere l'uso consapevole e critico da parte degli alunni oltreché prevenire le problematiche che derivano da un utilizzo non responsabile, pericoloso, dannoso o illegale delle tecnologie digitali.

Nella consapevolezza sia dei potenziali e sempre nuovi rischi connessi all'utilizzo della Rete, sia di avere il compito di formare il cittadino Digitale e che l'uso di dotazioni tecnologiche è

un'opportunità e non un diritto, l'Istituto si pone innanzitutto come ente di formazione, educazione, sensibilizzazione, corresponsabilizzazione e prevenzione, piuttosto che di inibizione e repressione.

Il presente documento potrà essere revisionato e aggiornato annualmente.

1. Tecnologie, metodologie e internet nella scuola di oggi.

La competenza digitale è una delle competenze chiave per l'apprendimento permanente, identificate dall'Unione Europea.

L'azione #6 del PNSD (Piano Nazionale Scuola Digitale) "Politiche attive per il BYOD" (Bring your own device), - letteralmente: porta il tuo dispositivo - punta a garantire a tutti gli studenti una formazione digitale che parta dal saper usare e usare consapevolmente i propri dispositivi.

"La scuola digitale, in collaborazione con le famiglie e gli enti locali, deve aprirsi al cosiddetto BYOD (Bring Your Own Device), ossia a politiche per cui l'utilizzo di dispositivi elettronici personali durante le attività didattiche sia possibile ed efficientemente integrato".

Tale indicazione è stata chiarita con i "Dieci punti per l'uso dei dispositivi mobili a scuola BYOD - Bring your own device" scaricabile [qui](#).

Poiché la tecnologia fornisce agli studenti opportunità innovative ed inedite per incrementare la loro cultura e le loro competenze, in linea con quanto specificato nel PNSD, il nostro Istituto intende favorire tale processo fondato sulla costruzione di un insegnamento basato sulla didattica laboratoriale, sullo sviluppo della capacità di risolvere problemi, sulla multimedialità, sulla centralità e individualità dello studente che apprende, con l'obiettivo di migliorare gli ambienti formativi utilizzando le tecnologie come strumenti per la promozione dei processi di apprendimento e sviluppare la produzione di materiali didattici diversificati, che promuovano l'attivazione di più linguaggi e codici comunicativi.

La scuola intende potenziare la competenza digitale degli studenti, intesa soprattutto come uso consapevole, critico e creativo delle tecnologie, per coglierne le valenze, ma anche i limiti e i rischi garantendo la sicurezza di tale processo attraverso una modalità di interazione, tra studenti, docenti e famiglie, che contribuisca al miglioramento dell'ambiente educativo e di apprendimento. Indicazioni metodologiche e progetti relativi sono parte integrante del PTOF di Istituto.

2. Rischi e opportunità della Rete

Numerose sono le tematiche connesse ad un uso consapevole delle tecnologie digitali: Identità, Privacy, Credibilità, Creatività, Collaborazione, Partecipazione, Apprendimento, Rispetto dei diritti d'autore... La scuola ritiene esaustiva la ricerca condotta da EU Kids linkata a seguito e riassunta nella tabella che segue. Ritiene altresì di prioritaria importanza la continua formazione e sensibilizzazione ad un uso corretto e consapevole delle TIC e della Rete per la formazione del Cittadino Digitale di domani.

[Link alla ricerca](#)

[Accesso, usi, rischi e opportunità di internet per i ragazzi italiani di EU Kids Online 2017](#)

TABELLA DEI RISCHI E DELLE OPPORTUNITA' OFFERTE DALLA RETE

	CONTENUTI	CONTATTI	CONDOTTA
RISCHI	Pericolosi o offensivi, falsi o non affidabili, pubblicità o spamming	Privacy, contatti con sconosciuti, episodi di cyberbullismo, tracciamento utente a fini commerciali	Pirateria, gioco d'azzardo, atti di bullismo, creare false identità
OPPORTUNITA'	Risorse per apprendimento e intrattenimento	Condivisione di interessi ed esperienze, partecipazione a community e social network	Espressione della propria identità online, creazione di contenuti, apprendimento collaborativo, partecipazione civica

Si ribadisce che registrazioni e riprese audio/foto/video sono consentite, nel rispetto dei regolamenti allegati, per uso personale, mentre la diffusione di tali contenuti è invece sempre subordinata al consenso da parte delle persone ritratte/riprese. Tale consenso dovrà essere rilasciato in forma scritta.

Si richiama l'attenzione degli alunni, dei docenti e delle famiglie sulle possibili conseguenze di eventuali riprese audio/video o fotografie effettuate all'interno degli ambienti scolastici, al di fuori dei casi consentiti, e successivamente diffuse con l'intento di ridicolizzare compagni o insegnanti o addirittura allo scopo di intraprendere azioni che sono spesso definite con il termine di cyberbullismo. Tali azioni possono configurare, nei casi più gravi, gli estremi di veri e propri reati.

3. Ruoli e Responsabilità

Dirigente scolastico	<ul style="list-style-type: none"> a. Perseguire la sicurezza online dei membri della comunità scolastica. b. Offrire ai docenti la possibilità di accedere ad una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della Comunicazione; c. Definire e rivedere periodicamente la E-Safety. d. Implementare l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line.
----------------------	--

	<ul style="list-style-type: none"> e. Essere a conoscenza e seguire le procedure previste dalle norme in caso di reclami o infrazioni della E-Safety. f. Coordinare e supervisionare il personale che collabora per la sicurezza online interna. g. Assicurarsi dell'adeguatezza e correttezza delle pubblicazioni sul sito web dell'Istituto, per quanto riguarda gli obblighi di pubblicazione previsti dalla normativa vigente. h. Individuare, in collaborazione con il DSGA, misure organizzative volte ad assicurare la regolarità e la tempestività dei flussi informativi.
<p>Direttore dei Servizi Generali e Amministrativi e/o personale nominato dal DS</p>	<ul style="list-style-type: none"> a. Assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per consentire che l'infrastruttura tecnica della scuola sia funzionante e sicura. b. Assicurare, nei limiti delle risorse finanziarie disponibili, l'acquisto delle risorse tecniche o software, oltre che delle strumentazioni didattiche, per la sicurezza e il funzionamento dei diversi canali di comunicazione della scuola all'interno della scuola e fra la scuola e le famiglie degli alunni. c. Fornire ai docenti, tramite gli assistenti amministrativi addetti, le password per l'accesso al registro elettronico. d. Fornire al personale di segreteria le utenze e le password personali per l'accesso ai pc, alle cartelle private sul Nas e ai gestionali in cloud (Nuvola, Mediasoft, SIDI). e. Verificare periodicamente il corretto aggiornamento automatico dei software antivirus e dei sistemi operativi sui pc della segreteria, dando indicazioni agli assistenti amministrativi sul corretto uso delle attrezzature, delle password, dei software e della rete internet. f. Coordinare l'attività degli assistenti amministrativi in merito alla pubblicazione dei vari documenti e curare, in collaborazione con il Dirigente Scolastico, l'aggiornamento delle informazioni già presenti sul sito web relativamente alle comunicazioni generali e alla pubblicazione dei documenti obbligatori per il sito istituzionale, previsti dalla normativa vigente.
<p>Animatore Digitale, TEAM per l'innovazione, PST e addetti alle strumentazioni tecnologiche</p>	<ul style="list-style-type: none"> a. Pubblicare e diffondere la E-Safety Policy. b. Stendere ed attuare il Piano Animatore Digitale. c. Promuovere la formazione interna all'istituzione. d. Coordinare e proporre attività didattiche e di formazione per personale e alunni. e. Monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche

	<p>dell'istituzione con l'eventuale individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola.</p> <p>f. Curare la manutenzione, l'aggiornamento e lo sviluppo del sito web della scuola per quanto riguarda l'area dedicata al settore didattico sul sito web.</p> <p>g. Coinvolgere la comunità scolastica (alunni, insegnanti, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti l'utilizzo della Rete e delle tecnologie.</p> <p>h. Gestire e monitorare gli account GSuite for Education di alunni e personale.</p> <p>i. Verificare periodicamente il corretto aggiornamento dei software antivirus e dei sistemi operativi delle strumentazioni.</p> <p>j. Intervenire adeguatamente in caso di mal funzionamento delle strumentazioni.</p>
<p>Referente Cyberbullismo</p>	<p>a. Organizzare la formazione/sensibilizzazione al problema.</p> <p>b. Collaborare con l'Animatore Digitale nella gestione della pagina del sito internet di Istituto dedicata.</p> <p>c. Coadiuvare il Dirigente Scolastico nella gestione dei casi problematici.</p> <p>d. Fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi.</p> <p>e. Coordinare e proporre attività didattiche e di formazione per personale e alunni.</p>
<p>Docenti</p>	<p>a. Informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di Internet e sulla politica di sicurezza adottata dalla scuola, rispettandone regolamenti e regolamentazioni.</p> <p>b. Integrare nel curriculum scolastico e nelle attività didattiche ed educative delle classi le modalità di utilizzo corretto e sicuro delle TIC e di internet.</p> <p>c. Formare gli alunni perché comprendano e seguano le linee guida per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet.</p> <p>d. Informare gli alunni sull'esistenza della Policy di E-Safety ed illustrare la parte che li riguarda.</p> <p>e. Assicurarsi che gli alunni e le famiglie abbiano preso visione dei vari documenti inerenti la Policy e la Privacy, controllando e tenendo ben presente i consensi accordati.</p> <p>f. Conservare in sicurezza i documenti firmati da alunni e genitori, in collaborazione con la segreteria.</p>

	<ul style="list-style-type: none"> g. Assicurare che gli alunni abbiano una buona comprensione delle opportunità offerte dalle tecnologie digitali e dalla rete, ma soprattutto divengano critici e consapevoli nell'utilizzo dei contenuti, nel rispetto della normativa sul diritto d'autore e sulla privacy e maturino quanto meglio la competenza per una cittadinanza digitale. h. Garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con modalità e sistemi istituzionali. i. Assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente. j. Guidare e supervisionare gli alunni durante le attività scolastiche nelle quali è programmato l'utilizzo di Internet. k. Ritirare i dispositivi personali o inibire l'uso di quelli della scuola nel caso si riscontrino irregolarità nell'utilizzo degli stessi durante l'orario scolastico e nel corso di tutte le attività ed iniziative di ampliamento dell'offerta formativa. l. Comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo. m. Segnalare eventuali problemi legati alla sicurezza e alla pulizia delle strumentazioni utilizzate o presenti in classe. n. Segnalare, all'Animatore Digitale, qualsiasi esigenza o proposta di carattere tecnico-organizzativo-informativo in materia di prevenzione e gestione dei rischi nell'uso delle TIC. o. Segnalare al Dirigente scolastico, al Referente del cyberbullismo e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di Internet, per l'adozione delle procedure previste dalle norme.
<p>Alunni</p>	<ul style="list-style-type: none"> a. Essere responsabili, in relazione al proprio grado di maturità e di apprendimento, dell'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti. b. Comprendere le potenzialità offerte dalle TIC per la ricerca di contenuti e materiali, ma anche la necessità di evitare il plagio e rispettare i diritti d'autore. c. Comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi. d. Adottare condotte rispettose degli altri anche quando si comunica in rete.

	<ul style="list-style-type: none"> e. Capire l'importanza di segnalare, bisogni, dubbi, abusi, uso improprio o accesso a materiali inappropriati. f. Assumersi la responsabilità delle strumentazioni personali o della scuola utilizzate.
Genitori	<ul style="list-style-type: none"> a. Conoscere e sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni (TIC) nella didattica. b. Controllare che gli alunni, nello studio a casa, adottino i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, con particolare riferimento all'utilizzo dei device e di internet. c. Collaborare con la scuola ad una educazione civica digitale del proprio figlio.

4. Gli spazi fisici e virtuali disponibili della scuola

Negli ultimi anni la scuola si è dotata di diversi strumenti tecnologici che mette pienamente a disposizione dell'utenza e del personale; consente la pratica del Byod (Bring your own device) e ne regola l'utilizzo.

Ogni plesso è dotato di connessione a banda larga.

La segreteria è dotata di un sistema di mirroring e backup e di una connessione a banda larga "privata".

I tre plessi di scuola primaria e il plesso di scuola secondaria sono dotati di firewall UMT con content filtering e logging. In tutte le classi sono presenti LIM.

I tre plessi di primaria posseggono 1 laboratorio informatico, 1 postazione docente, e una dotazione mobile di pc portatili utilizzati nelle classi e per la formazione del corpo docente. Un plesso scolastico di primaria è dotato di strumentazioni per la classe 2.0.

Ogni plesso ha a disposizione devices per gli alunni con difficoltà di apprendimento.

Presso la scuola secondaria è allestito 1 atelier CreAttivo, a disposizione di tutto l'Istituto, dotato di strumentazioni mobili quali tablet e pc portatili con carrello per la carica, strumentazioni per la robotica educativa, sperimentazioni elettriche ed elettroniche, il videomaking e la web radio.

La scuola secondaria possiede un laboratorio informatico, alcune postazioni mobili, un'aula di recupero dotata di postazioni fisse.

I tre plessi di scuola dell'infanzia sono dotati di postazioni mobili per i docenti e le famiglie.

Ogni plesso provvede alla stesura di una regolamentazione per l'utilizzo, la manutenzione e il corretto funzionamento nelle aule e delle postazioni informatiche, al fine di dare indicazioni di prassi opportune e invitare ad un uso sempre più professionale delle TIC da parte di tutto il personale scolastico.

Le apparecchiature presenti nella Scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto, minimizzando gli sprechi di risorse a disposizione (energia, carta, inchiostro, etc.).

Gli insegnanti sono responsabili delle TIC nell'ambito dell'attività didattica e hanno il compito di responsabilizzare gli alunni per divenire consapevoli dell'importanza della salvaguardia di un bene comune, seguendo le corrette norme di utilizzo (vedi regolamenti allegati).

Nell'Istituto sono stati individuati docenti incaricati della manutenzione delle apparecchiature e il TEAM, insieme all'Animatore Digitale, al supporto e alla formazione di alunni e docenti.

L'Istituto possiede un sito web <http://www.iccasalgrande.edu.it> dove vengono regolarmente pubblicati avvisi, atti, circolari e alcune attività didattiche.

L'Istituto fornisce, su richiesta degli insegnanti account GSuite a tutti gli alunni, previo consenso informato alle famiglie.

Ogni docente è dotato di un account GSuite di Istituto, che è utilizzato come mezzo prioritario di scambio di informazioni e collaborazioni.

L'Istituto utilizza il Registro Elettronico e la segreteria ha effettuato il passaggio alla digitalizzazione.

5. Strategie adottate per garantire la sicurezza delle TIC e pericoli della Rete

- Due sono le tipologie di accesso a Internet: docenti e alunni. Per la seconda sono attivate restrizioni e controlli maggiori.
- Gli account GSuite assegnati agli alunni hanno alcune restrizioni legate soprattutto ai social o agli esterni all'organizzazione.
- Attivazione percorsi di formazione/sensibilizzazione per un uso consapevole delle TIC rivolti ad alunni, insegnanti e famiglie.
- Realizzazione di percorsi di formazione/incontri con la Polizia Postale sui pericoli della rete e sull'uso corretto e consapevole della rete.
- Coinvolgimento dei genitori come partner educativi nei percorsi di formazione per il conseguimento delle competenze di cittadinanza digitale che riguardano gli studenti.
- Controllo del sistema informatico (cronologia, cookies, password personali per chiunque accede al sistema ecc.) e firewall per l'accesso ad Internet periodicamente aggiornato.
- Aggiornamento periodico del software antivirus e scansione delle macchine in caso di sospetta presenza di virus.
- La segreteria è dotata di un sistema di mirroring e backup.

6. Norme comportamentali dell'utente

La scuola richiede il rispetto per la normativa vigente in fatto di diritti, sicurezza e privacy*, delle norme di netiquette e buona educazione, e dei regolamenti interni, relativi all'utilizzo dell'apparato tecnologico, di cui si è dotata (vedi paragrafo successivo).

L'Istituto mette a disposizione degli utenti (alunni, personale, insegnanti...) le proprie strumentazioni e consente, laddove la si ritiene opportuna ed efficace, la pratica del Byod richiedendo il rispetto, da parte degli utenti, delle seguenti norme di comportamento:

- rispetto del regolamento Byod e della regola del semaforo ad esso allegata;
- cura della sicurezza dei propri e altrui dispositivi;
- divieto di aprire o distribuire file infetti o danneggiati o di non sicura provenienza;
- comunicazione all'insegnante o al personale scolastico di comportamenti anomali o dubbi che facciano presupporre la presenza di danno presunto (malware, spyware, virus...);

- rispetto dei regolamenti interni e della legislazione vigente in termini di sicurezza, privacy e diritti d'autore;
- tutela della propria privacy, di quella degli altri utenti non divulgando dati sensibili, foto o video senza il consenso dell'interessato o del suo tutore;
- rispetto della cosiddetta netiquette (regole condivise che disciplinano la comunicazione fra utenti della rete, wiki, siti, forum, mail, messaggistiche, social...).

7. Documentazioni, Regolamenti, gestione dei casi

ALLEGATI

1. Consenso/Informativa attivazione e autorizzazione consegna GSuite 1A personale - 1B alunni - 1C alunni (a cura di RPD o DPO)
2. Regolamento per l'uso dei telefoni cellulari e dispositivi mobili da parte degli alunni a scuola - gestione dei casi
3. Patto/Regolamento Byod
4. Utilizzo strumentazione tecnologica della scuola
5. Liberatoria foto-video (a cura di RPD o DPO)
6. Piccola guida di cittadinanza
7. Liberatoria opere dell'ingegno di carattere creativo

[*Vademecum Garante Privacy](#)

[Regolamento UE 2016/679 sulla protezione dei dati](#)

[Guida all'applicazione del Regolamento Europeo in materia di protezione dei dati personali - Garante Privacy](#)

[Dichiarazione dei diritti in Internet - Camera dei Deputati](#)