ISTITUTO COMPRENSIVO
CARDITO IC 2 "DON BOSCO"
Via Taverna – 80024 Cardito (Na)
Tel. 0818348455 – Fax 0818348326
Cod Meccanografico NAIC8GM00E
C.F. 93066110631
E-mail: naic8gm00e@istruzione.it
Pec: naic8gm00e@pec.istruzione.it
http://www.carditoic2donbosco.gov.it

E-Policy sull'utilizzo delle TIC

A.S. 2016/17

Finalità del documento

L' e-policy d'istituto ha lo scopo di fornire le linee guida essenziali per l'utilizzo corretto e sicuro delle apparecchiature informatiche in dotazione alla scuola, sia da parte degli alunni che del personale docente e non docente. L'e-policy ha altresì lo scopo di promuovere un uso corretto e sicuro dei dispositivi informatici di proprietà degli alunni e del personale (smartphone, tablet, laptop) divenuti parte essenziale della quotidianità didattica, lavorativa e ludica della società odierna, ma anche potenziale veicolo di pericoli di diversa natura cui, purtroppo, l'utente medio, bambino o adulto che sia, non è sufficientemente preparato. Negli ultimi anni, infatti, la familiarità delle nuove generazioni con le tecnologie informatiche, la rapidità con cui esse hanno imparato prima a digitare che a scrivere con carta e penna, hanno alimentato l'illusione che i *nativi digitali* fossero in grado di orientarsi da soli nel mare magnum del mondo virtuale. In realtà Le TIC, e in particolare Internet, rappresentano un medium di *informazione* ormai imprescindibile, ma la quantità di dati che esse offrono non si traducono immediatamente in *formazione*, cioè competenze nella gestione delle informazioni stesse, capacità di vagliarle criticamente, formazione di una pensiero complesso. Compito della scuola, dunque, non è solo fornire indicazione operative nell'uso materiale delle TIC, ma anche e soprattutto promuovere una riflessione di tipo *etico* su tale utilizzo, che il mezzo in sé non può fornire, soprattutto in relazione alla sicurezza, alla salvaguardia dei dati personali, alla costruzione consapevole di un'identità digitale.

Ruoli e Responsabilità

DIRIGENTE SCOLASTICO

- Promuovere e garantire la sicurezza dei membri della comunità scolastica nell'uso delle TIC
- Promuovere la formazione e l'aggiornamento dei docenti e del personale non docente nell'uso consapevole delle tecnologie informatiche
- Garantire l'esistenza e il funzionamento del sistema di monitoraggio dell'uso delle TIC
- Gestire reclami e attribuzioni di responsabilità in caso di uso improprio delle TIC

ANIMATORE DIGITALE

- Stimolare la formazione di una comunità digitale e offrire consulenza al personale in relazione alle problematiche inerenti le TIC
- Monitorare globalmente l'utilizzo delle TIC, segnalare i problemi emergenti, proporre revisioni migliorative della policy in relazione alle mutate esigenze dell'istituto
- Manutenzione delle password e monitoraggio degli accessi dai computer della scuola
- Aggiornamento e manutenzione del sito internet e degli altri canali di presenza della scuola in rete
- Coinvolgere il contesto sociale (genitori e altre istituzioni del territorio) in un progetto comunità digitale

DSGA

- Garantire il funzionamento delle TIC attraverso interventi di personale specializzato, nei limiti delle risorse finanziarie disponibili
- Garantire il funzionamento dei canali di presenza della scuola in rete e l'accesso alla documentazione on line

DOCENTI

- Diritto/dovere di formarsi e aggiornarsi nel campo delle tecnologie digitali e del loro uso nella didattica

- Includere nei progetti didattici elementi di alfabetizzazione informatica sia a livello operativo che di riflessione sul corretto utilizzo delle stesse
- Monitorare l'utilizzo delle TIC da parte degli alunni durante l'orario scolastico
- Promuovere la comunicazione digitale con alunni e famiglie attraverso opportuni ambienti virtuali (Classi virtuali, piattaforme di e-learning ecc.)
- Rilevare e denunciare tempestivamente comportamenti pericolosi o utilizzi impropri delle TIC da parte degli alunni, sia di quelle in dotazione all'istituto, sia quelle in possesso degli alunni stessi
- Offrire guide e sitografie sugli argomenti di studio, promuovendo un vaglio critico delle fonti
- Proporre interventi migliorativi nella gestione delle TIC all'Animatore Digitale

ALUNNI
- Comprendere di essere responsabili dell'utilizzo delle risorse di rete della scuola
- Utilizzo consapevole dei contenuti reperiti in rete, anche in relazione alla salvaguardia del diritto d'autore
- Imparare e adoperare le buone pratiche di sicurezza in rete
- Comprendere i criteri di comunicazione non violenta in reta
- Esprimere i propri bisogni educativi nel campo dell'utilizzo delle TIC

Condivisione e pubblicizzazione della e-policy

Precipua finalità dell'istituzione è la massima condivisione delle presenti linee guida agli alunni, ai genitori e al personale della scuola. A tal fine:
- Il documento sarà discusso in sede di collegio, comunicato a tutto il personale, agli alunni e ai genitori, e reso disponibile su tutti i canali web
- Il personale e gli alunni saranno informati sul monitoraggio delle attività svolte in rete e dei sistemi di filtraggio adottati dalla scuola
- La formazione nell'uso delle TIC precederà sempre il loro effettivo utilizzo
- L'elenco delle regole da seguire sarà affisso nei luoghi di fruizione delle tecnologie informatiche
- Tutto il personale, gli alunni e i genitori saranno informati adeguatamente sulla sanzionabilità di condotte non conformi alla policy d'istituto

Infrazioni della policy e sanzioni

Il ricorso a comportamenti non conformi alla presente policy da parte degli attori coinvolti comporta il ricorso a sanzioni disciplinari la cui severità sarà correlata alla gravità dell'infrazione. L'intento della sanzione non sarà puramente punitivo, ma servirà come momento di riflessione sul proprio operato e per la correzione di condotte pericolose per sé e per gli altri.

In particolare, i comportamenti sanzionabili comprendono:
- Utilizzo dell'*hate speech*
- Infrazioni della *netiquette*
- Invio e ricezione di materiale fotografico, video o sonoro senza il consenso dei protagonisti
- Violazioni della privacy
- Comunicazione con sconosciuti
- Utilizzo di applicazioni o siti non autorizzati

Le sanzioni, nel caso degli alunni, saranno le stesse previste per comportamenti scorretti in altri campi, dal semplice richiamo verbale alla convocazione dei genitori e possibile sospensione dell'alunno resosi colpevole di condotte particolarmente rischiose e violente (cyber bullismo).

Nel caso del personale scolastico le condotte sanzionabili includono:

- Utilizzo dell'attrezzatura informatica per fini personali
- Trattamento dei dati personali e dei dati sensibili non in conformità con la legge vigente in materia
- Carenze nella formazione/autoformazione
- Carenze nella formazione degli alunni
- Interventi correttivi insufficienti
- Mancata vigilanza

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, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

Monitoraggio e revisione e-policy

Il monitoraggio dell'implementazione della policy e del suo eventuale aggiornamento sarà svolta ogni anno. Tale monitoraggio sarà curato dal Dirigente scolastico con la collaborazione dell'Animatore digitale e dai docenti delle classi. L'aggiornamento della policy sarà curato dal Dirigente scolastico, dall'Animatore digitale, dagli Organi Collegiali, a seconda degli aspetti considerati.

Utilizzo dei laboratori informatici

1. Le apparecchiature sono di proprietà della scuola e vanno pertanto utilizzate con cautela e rispetto
2. Il laboratorio informatico può essere usato solo a fine didattico o di aggiornamento degli alunni e del personale
3. E' obbligatorio registrare l'utilizzo del laboratorio su un apposito registro di prenotazione
4. L'ingresso agli alunni è consentito solo in presenza del personale docente
5. Il docente è responsabile dell'utilizzo di hardware e software
6. Le memorie esterne di proprietà degli alunni o del personale devono essere obbligatoriamente controllate con apposito antivirus
7. E' vietato alterare o cancellare file presenti sulle macchine, e altresì scaricare o disinstallare software senza previa autorizzazione
8. Il laboratorio va lasciato in ordine e con le macchine spente seguendo le procedure di arresto standard
9. Avvisare l'animatore digitale o il Dirigente Scolastico tempestivamente in caso di malfunzionamento
10. Salvare i dati importanti su memorie di back up
11. I software installati sono ad esclusivo uso didattico e non sono disponibili per prestiti individuali, se non dietro motivata e dettagliata richiesta da parte di un docente.
12. I software non devono violare le leggi sul copyright.
13. Le copie dei software o dei file non devono infrangere le leggi sul copyright

14. 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
15. Internet non può essere usato per scopi vietati dalla legislazione vigente
16. L’utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l’uso fatto del servizio Interne
17. E’ vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza.

Norme sull’uso di apparecchi telefonici nell’istituto

- L’utilizzo del telefono cellulare, dello smartphone e del tablet a scuola è severamente vietato, se non diversamente specificato dall’insegnante a solo fine didattico. Nel caso in cui l’alunno ne sia in possesso, esso dovrà essere tenuto nello zaino o in tasca spento. L’alunno sorpreso ad utilizzare il cellulare o lo smartphone subirà la requisizione dello stesso, che sarà posto in custodia dell’insegnante fino al termine delle lezioni.
- L’alunno e i genitori si assumono piena responsabilità dell’utilizzo improprio dei dispositivi cellulari (invio e ricezione di materiale audiovisivo senza autorizzazione, ecc.)
- La scuola non ha e non si assume responsabilità sulla custodia dei dispositivi di proprietà degli alunni in relazione all’uso improprio o al furto/smarrimento degli stessi
- L’accesso a internet su smartphone e tablet è regolato dalle medesime norme di accesso da PC fisso

Sicurezza in rete

Il rischio maggiore relativo all’uso improprio delle TIC consiste nelle minacce della rete: in un mondo sempre più connesso, si affacciano infatti quotidianamente diversi tipi di potenziali pericoli per l’utente finale, dalla clonazione della propria identità digitale ai fenomeni di phishing, cyber bullismo, stalking on line e adescamento di minori. Le linee guida per la prevenzione di tale rischio comprendono:

PREVENZIONE

- Informare e formare i docenti, i genitori, il personale ATA e gli studenti 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 alunni eccedenti i trattamenti istituzionali obbligatori
- Non consentire l’utilizzo del cellulare personale degli alunni 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
- Consentire l’utilizzo del cellulare sono in casi particolari ed eccezionali, ad esempio quando ci si trova fuori dal contesto scolastico durante una visita guidata, e comunque sotto la supervisione dell’insegnante, che si accerta preventivamente dell’identità dell’interlocutore
- Utilizzare filtri, software che impediscono il collegamento ai siti web per adulti (black list)
- Centralizzare il blocco dei siti web sul server del docente con appositi software

CONTENIMENTO

- Se la condotta incauta dell’alunno consiste nel fare circolare immagini imbarazzanti, di natura sessuale, su internet, è necessario rimuoverle: contattare il service provider e se il materiale postato viola i termini e le condizioni d’uso del sito chiedere di rimuoverle.

- Se l'alunno 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 o suggerirgli di bloccare o ignorare particolari mittenti, di cancellare il loro nominativo dalla lista degli amici con i quali regolarmente chatta, di inserire il compagno o la persona che offende, per quanto riguarda l'e-mail, tra gli indesiderati

- Consigliare di cambiare il proprio indirizzo e-mail, contattando l'e-mail provider, di scaricare un'applicazione che blocchi chiamate e messaggi da numeri indesiderati o, se necessario, cambiare il numero di cellulare contattando l'operatore telefonico

- Fare cancellare il materiale offensivo dal telefonino, facendo intervenire i genitori, e chiedere agli studenti 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.

RILEVAZIONE

Particolare importanza riveste la rilevazione di situazioni a rischio, non sempre facilmente individuabili per la reticenza dell'alunno che ne è vittima a confidarsi con genitori e insegnati. Un alunno che si mostra triste, ansioso, che ha un mutamento repentino nella condotta, ha atteggiamento evitante, si assenta spesso e ha un calo di rendimento potrebbe essere vittima di una situazione di stress originatasi on line che possono comprendere:

- ✓ Violazioni della privacy
- ✓ Contenuti offensivi o violenti
- ✓ Contenuti di natura sessuale

La segnalazione di casi di abuso deve essere corredata da prove prodotte dallo stesso alunno (messaggi in rete, foto, audio) o rintracciabili sui PC dell'istituto. Anche in assenza di prove, la denuncia da parte di un alunno va comunque notificata ai genitori e al DS, e, nei casi specifici, alla polizia. Per le segnalazioni di fatti rilevati sono previsti i seguenti strumenti che i 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 alunni, da parte dei docenti
- ✓ Relazione scritta al Dirigente scolastico.

LINEE GUIDA PER LA GESTIONE DEI CASI A RISCHIO

ALUNNI

- 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 in ogni caso chiedi sempre il permesso prima di pubblicare foto non tue
- Chiedi sempre al tuo insegnante a scuola o ai tuoi genitori a casa il permesso di scaricare documenti da Internet
- Non rispondere alle offese ed agli insulti
- Blocca gli utenti molestatori
- Se ricevi materiale offensivo (e-mail, sms, mms, video, foto, messaggi vocali) non diffonderlo:potresti essere accusato di cyber bullismo
- Conserva le comunicazioni offensive, ti potrebbero essere utili per dimostrare quanto ti è accaduto
- Riferisci al tuo insegnante o ai tuoi genitori se qualcuno ti invia immagini che ti infastidiscono e non rispondere
- Se qualcuno su Internet ti chiede un incontro di persona, riferiscilo al tuo 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 scaricare (download) o copiare materiale da Internet senza il permesso del tuo insegnante o dei tuoi genitori

INSEGNANTI

- Discutete con gli alunni 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
- Ricordate agli alunni che la violazione consapevole della policy e-safety della scuola, di utilizzo consentito della rete, comporta sanzioni di diverso tipo
- Adottate interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi
- 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 (sportello di ascolto psicologico gratuito attualmente attivo presso la scuola, Servizi Sociali per la fruizione di servizi socio-educativi comunali, ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare)
- 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 colleghi di classe e il Dirigente Scolastico, denunciate all'autorità giudiziaria o agli organi di Polizia

GENITORI

- 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 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 figlio 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 on-line di alta qualità: ricercare informazioni scientifiche, ricercare nuovi amici nel mondo
- Partecipa alle esperienze on-line: naviga insieme a tuo figlio, incontra amici on-line, discuti gli eventuali problemi che si presentano
- Comunicate elettronicamente con vostro figlio: inviate, frequentemente, E-mail, Instant Message
- Spiegate a vostro figlio 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 figlio a dirvi se vedono immagini particolari o se ricevono e-mail indesiderate
- Discutete nei dettagli le conseguenze che potranno esserci se vostro figlio visita deliberatamente siti non adatti, ma non rimproveratelo se compie azioni involontarie
- Spiegate a vostro figlio 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 figlio che non tutti in Internet sono chi realmente dichiarano di essere; di conseguenza i vostri ragazzi non dovrebbero mai accordarsi per appuntamenti senza consultarvi prima
- Il modo migliore per proteggere vostro figlio è usare Internet con loro, discutere e riconoscere insieme i rischi potenziali.

Il Dirigente Scolastico
Dott.ssa Lucia Signoriello
Firma autografa sostituita a mezzo stampa ai sensi dell'art. 3, co. 2, DL.vo39/1993