ISTITUTO COMPRENSIVO "DON L. MILANI"

Codice Meccanografico
CLIC830004
Codice Univoco
UF1UIV

Via Filippo Turati s.n. – Caltanissetta (CL)
Tel 0934 598587 – Fax 0934 598008
e-mail: clic830004@istruzione.it
clic830004@pec.istruzione.it
www.icdonmilanicl.edu.it

Codice Fiscale
92062090854
Codice IPA
icdlm

REGOLAMENTO

Gestione dei dispositivi informatici dell'Istituto e degli strumenti multimediali (dispositivi, rete, Internet, mail, ecc.)

1. Introduzione

Il personale scolastico e gli studenti (di seguito indicati come utenti) che all'inizio dell'anno scolastico riceveranno in dotazione un netbook/tablet, dovranno scrupolosamente seguire le seguenti norme di comportamento e di manutenzione con riferimento alla strumentazione fornita in dotazione.

Il trattamento dei dati mediante l'uso di tecnologie telematiche è conformato al rispetto dei diritti e delle libertà fondamentali nonché della dignità dell'interessato. Ogni utente è responsabile, sia sotto il profilo civile che penale, del corretto uso delle risorse informatiche, dei servizi e dei programmi ai quali ha accesso e dei dati che tratta. Spetta ai docenti vigilare affinché gli studenti loro affidati rispettino il presente regolamento.

A scuola, le strumentazioni informatiche, la rete internet e la posta elettronica devono essere utilizzati unicamente come strumenti di lavoro e di studio. Ogni loro utilizzo non inerente all'attività lavorativa e di studio è vietato in quanto può comportare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. In particolare non può essere dislocato nelle aree di condivisione della rete alcun file che non sia legato all'attività lavorativa, nemmeno per brevi periodi.

Agli utenti è assolutamente vietata la memorizzazione di documenti informatici di natura oltraggiosa o discriminatoria per sesso, lingua, religione, razza, origine etnica, condizioni di salute, opinioni di appartenenza sindacale e politica.

Non è consentito scaricare, scambiare o utilizzare materiale coperto dal diritto d'autore.

In merito all'uso dei dispositivi personali delle studentesse e degli studenti in classe, la scuola, si riserva di implementare il presente documento, appena sarà aggiornato ***il piano scuola digitale nazionale***.

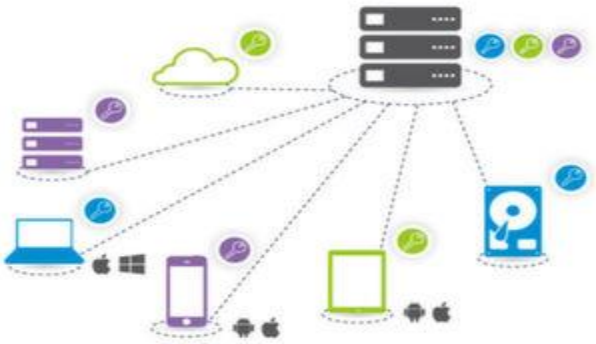
Lo scopo del presente regolamento è di:
stabilire i principi fondamentali che tutti i membri della comunità scolastica devono seguire nell'utilizzo di tecnologie; salvaguardare e proteggere i bambini, i ragazzi e lo staff dell'Istituto; impostare chiare aspettative di comportamento e/o codici di condotta rilevanti per un uso responsabile di Internet a scopo didattico, personale o ricreativo; prevenire casi di abusi online come il cyerbullismo; garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che il comportamento illecito o pericoloso è inaccettabile e che saranno intraprese le opportune azioni disciplinari e giudiziarie.

2. Gestione dell'infrastruttura e della strumentazione ICT della scuola.

Accesso ad internet: filtri antivirus e sulla navigazione.

La rete wi-fi o cablata dell'Istituto deve essere utilizzata con prudenza e diligenza. E' vietato scaricare software, musica, filmati, immagini illegali o vietati ai minori. Ogni utente è responsabile dell'utilizzo della rete e si impegna a mantenere segrete e a non comunicare a terzi le password d'ingresso della rete ed ai programmi e a non permettere ad alcuno di utilizzare il proprio accesso. Infine occorre preventivamente scansionare con antivirus ogni archivio elettronico (file) acquisito attraverso qualsiasi supporto (es. pen drive) prima di trasferirlo su aree comuni della rete. Agli utenti è fatto espresso divieto di influenzare negativamente la regolare operatività della rete, interferire con la connettività altrui o con il funzionamento del sistema e quindi di:
a. Utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files e software di altri utenti, utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di intercettazione di tastiera (keygrabber o keylogger), software di decodifica password (cracker) e più in generale software rivolti alla violazione della sicurezza del sistema e della privacy.
b. Sostituirsi a qualcuno nell'uso dei sistemi, cercare di catturare password altrui o forzare password o comunicazioni criptate.
c. Modificare le configurazioni impostate dall'amministratore di sistema.
d. Limitare o negare l'accesso al sistema a utenti legittimi.
e. Effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc.)
f. Distruggere o alterare dati altrui.
g. Usare l'anonimato o servirsi di risorse che consentano di restare anonimi.

Uso dei laboratori e dei dispositivi - Gestione accessi (password, backup, ecc.).



E’ vietato consumare cibi o bevande nei laboratori.
Gli utenti devono trattare con particolare cura i supporti magnetici (chiavi USB, CD riscrivibili, ecc.), in particolar modo quelli riutilizzabili, per evitare che persone non autorizzate possano accedere ai dati ivi contenuti.
L’accesso alla navigazione in Internet deve essere effettuato esclusivamente a mezzo della rete di Istituto e solo per fini scolastici. E’ tassativamente vietato l’utilizzo di modem personali. Gli utenti sono tenuti a utilizzare l’accesso a Internet in modo conforme a quanto stabilito dal presente regolamento e quindi devono:
a. Navigare in Internet in siti attinenti allo svolgimento delle mansioni assegnate.
b. Registrarsi solo a siti con contenuti legati all’attività didattica.
c. Partecipare a forum o utilizzare chat solo per motivi strettamente attinenti all’attività scolastica.
Agli utenti è fatto espresso divieto di qualsiasi uso di Internet che possa in qualche modo recare danno all’Istituto o a terzi e quindi di:
a. Fare conoscere ad altri la password del proprio accesso
b. Usare Internet per motivi personali
c. Servirsi dell’accesso Internet per attività in violazione del diritto d’autore o di altri diritti tutelati dalla normativa vigente.
d. Accedere a siti pornografici, di intrattenimento, giochi d’azzardo, ecc.
e. Utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer.
f. Ascoltare la radio o guardare video o filmati non autorizzati utilizzando le risorse Internet.
g. Effettuare transazioni finanziarie, operazioni di remote banking, acquisti on-line e simili, se non attinenti all’attività scolastica o direttamente autorizzati dal Dirigente Scolastico.
h. Inviare fotografie, dati personali o di terzi dalle postazioni Internet.
i. Effettuare spedizioni, a nome della scuola, di messaggi o file non autorizzati dal Dirigente Scolastico.

E-mail.

Gli utenti che utilizzano una casella di posta elettronica condivisa o uno spazio web remoto condiviso (comunque preventivamente autorizzato), sono responsabili del corretto utilizzo degli stessi e sono tenuti a utilizzarli in modo conforme a quanto stabilito dal seguente regolamento, quindi devono:

a. Conservare la password nella massima riservatezza e con la massima diligenza.

b. Mantenere in ordine la casella di posta o lo spazio web remoto, razionando opportunamente lo spazio di memorizzazione a disposizione.

c. Prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura e, dove possibile, preferire l'utilizzo di cartelle di rete condivise.

d. Inviare preferibilmente file in formato pdf.

e. Accertarsi dell'identità del mittente e controllare a mezzo di software antivirus gli allegati di posta elettronica prima del loro utilizzo.

f. Rispondere alle e-mail pervenute solo da emittenti conosciuti e avvisare il docente se si riscontra la presenza di file sospetti.

g. Chiamare link contenuti all'interno di messaggi solo quando vi sia la comprovata sicurezza sul contenuto dei siti richiamati.

Agli utenti è fatto espresso divieto di qualsiasi uso della posta elettronica che possa in qualche modo recare danno all'Istituto o a terzi e quindi di:

a. Prendere visione della posta altrui.

b. Simulare l'identità di un altro utente, ovvero utilizzare per l'invio di messaggi credenziali di posta non proprie, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza.

c. Utilizzare strumenti software o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all'interno dell'Istituto.

d. Trasmettere a mezzo posta elettronica, o remote drive, dati sensibili, personali o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento della protezione dei dati personali. e. Inviare tramite posta elettronica, o remote drive, user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici.

f. Utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione.

g. Inviare o ricevere posta personale attraverso l'uso di un webmail.

h. Utilizzare il servizio di posta elettronica per inoltrare giochi, scherzi, barzellette, appelli e petizioni, messaggi tipo "catene" e altre e-mail che non siano attinenti all'attività scolastica.

Blog e sito web della scuola

L'Istituto dispone di un proprio spazio Web e di un proprio dominio: Istituto Comprensivo "Don L. Milani" Caltanissetta.

L'Istituto gestisce un proprio sito web nello spazio di proprietà. La gestione del sito della scuola e la rispondenza alle normative per quanto concerne i contenuti (accuratezza, appropriatezza, aggiornamento) e le tecniche di realizzazione e progettazione è a cura del Webmaster. La scuola detiene i diritti d'autore dei documenti che si trovano sul proprio sito o di quei documenti per i quali è stato chiesto ed ottenuto il permesso dall'autore proprietario. Le informazioni pubblicate sul sito della scuola relative alle persone da contattare rispetteranno le norme vigenti sulla privacy.

La scuola, in qualità di ente pubblico, pubblicherà sul proprio sito web i contenuti che saranno valutati come pertinenti alle finalità educative istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative.

Social network.

L'Istituto dispone di una pagina su Facebook: https://www.facebook.com/istitutocomprensivodonlmilani/?ref=br_rs

La scuola detiene i diritti d'autore dei documenti che si trovano sulla pagina Facebook o di quei documenti per i quali è stato chiesto ed ottenuto il permesso dall'autore proprietario. La scuola, in qualità di ente pubblico, pubblicherà sulla propria pagina Facebook i contenuti che saranno valutati come pertinenti alle finalità educative istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative.

Protezione dei dati personali.

E' vietato eseguire, negli ambienti scolastici, filmati o fotografie non autorizzati dal Dirigente Scolastico.

E' altresì vietata la diffusione del suddetto materiale sia in formato cartaceo che telematico. È fatto divieto assoluto di effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi. E' possibile registrare la lezione esclusivamente per motivi di studio individuale e a scopo personale solo con il consenso del docente presente. Per ogni altro utilizzo, anche didattico, o eventuale diffusione, anche su Internet, è necessario informare preventivamente e adeguatamente il Dirigente Scolastico, le persone coinvolte nella registrazione (professori, studenti...), e ottenere l'esplicito consenso, libero, informato e preventivo, delle persone interessate.

L'Istituto dispone di un dominio su rete locale (rete segreteria) cui accedono i Computer dell'amministrazione. Tali postazioni sono su una rete locale isolata dal resto della rete d'Istituto (rete didattica). Il Collegamento di computer portatili o palmari personali alla rete di Istituto deve essere

autorizzato dal Dirigente Scolastico. La rete interna è protetta da Firewall per quanto riguarda le connessioni con l'esterno. Le postazioni sono protette con sistemi antivirus regolarmente aggiornati.
L'Istituto dispone di una rete con tecnologia senza fili. L'accesso alla rete wireless è regolato da un controller che determina l'accesso degli utenti, docenti e studenti, tramite il riconoscimento del dispositivo utilizzato. L'ottenimento delle credenziali è riservato a personale dell'Istituto e ospiti. Le regole di comportamento sono analoghe a quelle per la connessione alle reti cablate di Istituto.

Si ricorda inoltre che il Garante della Privacy ha emesso il 10 giugno 2010 un vademecum per la sicurezza e la privacy nelle scuole, mentre dal 6 settembre 2012 vige un memorandum contenente le indicazioni inerenti l'utilizzo di tablet, smartphone, pc, ecc. In particolare il Garante ricorda l'uso strettamente personale degli smartphone, nel rispetto della persona e che ogni Istituto scolastico decide, nella propria autonomia, la regolamentazione nell'uso di cellulari e tablet. Comunque sottolinea che non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese. Si ricorda che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere lo studente in sanzioni disciplinari e pecuniarie nonché in responsabilità civile e penale. Le stesse cautele valgono per l'uso dei tablet, se usati a fini di registrazione e non soltanto per fini didattici o per consultare in classe libri elettronici e testi on line (documento emanato il 6 settembre 2012). "Inoltre va prestata attenzione alla eventuale pubblicazione delle immagini su internet e sui social network in particolare. In caso di comunicazione sistematica o diffusione diventa, infatti, necessario di regola ottenere il consenso delle persone presenti nelle fotografie e nel video. Non è possibile in ogni caso diffondere o comunicare sistematicamente i dati personali di altre persone (ad esempio immagini o registrazioni audio/video) senza aver prima informato adeguatamente le persone coinvolte e averne ottenuto l'esplicito consenso" (documento del 10 giugno 2010)

3. Strumentazione personale

Per studenti, docenti e personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc..

I telefoni cellulari possono essere utilizzati durante l'orario scolastico esclusivamente per scopi didattici dietro autorizzazione del DS in base a quanto previsto dal PNSD. Gli altri devices possono essere utilizzati dagli alunni in classe solo se autorizzati, alla presenza del docente e per ragioni prettamente scolastiche.
Se – malgrado il divieto appena espresso – gli studenti verranno sorpresi ad usare il cellulare, lo stesso

verrà temporaneamente requisito dai docenti che registreranno l'episodio sul registro di classe e – in collaborazione con il personale ausiliario e/o con la segreteria – convocheranno per le vie brevi i genitori interessati ai quali verrà riconsegnato il cellulare requisito. Avuto inoltre riguardo per il fatto che i moderni cellulari possono essere utilizzati anche per scattare foto (o effettuare riprese filmate) e per trasferirle con un MMS chissà a chi e chissà dove, si informano i Sigg. genitori che eventi di questo tipo – se si concretizzano durante l'orario scolastico – si possono configurare anche come reati per i quali non si esclude la segnalazione ai competenti organi di Pubblica Sicurezza

I docenti e il personale della scuola non possono utilizzare cellulari e tablet a scopo personale durante l'attività didattica o lavorativa.

Ogni utente è personalmente responsabile della custodia della strumentazione fornita in dotazione e del materiale consegnatogli; è tenuto al risarcimento dei danni causati da comportamenti contrari a quanto stabilito dal presente regolamento.
Ogni utente è responsabile della custodia del dispositivo affidatogli sia nei locali della scuola che in ambienti ad essa esterni, le apparecchiature non devono essere mai lasciate incustodite. In particolare egli deve applicare al pc portatile/tablet le regole di utilizzo previste per i pc connessi in rete. Deve custodirlo con diligenza e in luogo protetto durante gli spostamenti. Deve rimuovere gli eventuali file elaborati sullo stesso, prima della sua riconsegna all'Istituto.
Gli utenti sono responsabili di rotture e/o disfunzioni delle attrezzature causate da scorretto utilizzo delle stesse. Coloro che, provocano dolosamente o colposamente danni alle attrezzature e/o apparecchiature, dell'aula o del laboratorio sono soggetti a sanzioni disciplinari, nel caso dello studente, e sono tenuti al risarcimento del danno.
Eventuali guasti, rotture o ammanchi devono essere segnalati da parte del docente responsabile sull'apposito "registro guasti".
Non è possibile eseguire operazioni di manutenzione ordinaria o straordinaria autonomamente. In caso di guasto software/hardware, gli studenti dovranno rivolgersi al docente che provvederà a far riparare il dispositivo e a segnalare la riparazione sul registro guasti.
Non è possibile rimuovere dall'aula il materiale in esso presente, senza autorizzazione del Dirigente Scolastico.
Il docente dell'ultima ora provvede a ritirare nell'apposita posizione il materiale utilizzato.
La strumentazione fornita in dotazione deve essere riconsegnata integra alla fine delle attività previste, in accordo con i docenti del C.d.C, nel caso dello studente, e col Dirigente Scolastico, nel caso del personale della scuola.

Gli utenti che utilizzano pc/tablet di proprietà dell'Istituto scolastico, salvo espresse autorizzazioni, sono tenuti a:
a. Attivare sul PC lo screen saver e la relativa password.
b. Conservare la password nella massima riservatezza e con la massima diligenza, consegnare la stessa in segreteria (in busta chiusa).
c. Non inserire password che non rendano accessibile il computer al personale scolastico, se non esplicitamente autorizzato (come da registrazione sulla scheda del dispositivo).
d. Non utilizzare cripto sistemi o qualsiasi altro programma di sicurezza crittografica non previsto esplicitamente dal docente responsabile (funzione strumentale).
e. Non modificare la configurazione hardware e software del proprio PC/tablet, se non esplicitamente autorizzati dai docenti (come da apposito registro).
f. Non rimuovere, danneggiare, o asportare componenti hardware e sigilli di garanzia.
g. Non installare sul pc dispositivi hardware personali (modem, schede audio, masterizzatori, pendrive, dischi esterni, i-pod, telefoni, ecc.) salvo specifica autorizzazione in tal senso da parte del docente (come da apposito registro).
h. Gli studenti non possono installare autonomamente software, se non esplicitamente autorizzati dal docente (come da apposito registro software).
i. Non utilizzare programmi non autorizzati.

j. Prestare la massima attenzione ai supporti di origine esterna (es. pen drive), verificando preventivamente tramite il programma di antivirus ogni file acquisito attraverso qualsiasi supporto e avvertire immediatamente il docente responsabile o il responsabile di plesso nel caso in cui vengano rilevati virus.
k. Non lasciare incustodita ed accessibile la propria postazione o il proprio dispositivo una volta connesso al sistema con le proprie credenziali di autenticazione.
l. Non cedere, una volta superata la fase di autenticazione, l'uso del proprio dispositivo a persone non autorizzate, in particolar modo, per quanto riguarda l'accesso a Internet e ai servizi di posta elettronica.
m. Spegnere il pc/tablet al termine del lavoro o in caso di assenze prolungate dalla propria postazione.
n. Non è possibile scambiarsi i dispositivi assegnati o prestarli a terzi.
o. E' vietato duplicare software protetto da copyright. Non è possibile eliminare software senza il permesso del docente. L'eliminazione deve essere segnalata sull'apposito registro a cura del docente.
p. E' assolutamente vietato effettuare jailbreak sui tablet.

5. Prevenzione dei casi

Rischi

I rischi effettivi che si possono correre a scuola nell'utilizzo delle TIC da parte degli alunni 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 alunni soprattutto per mantenere la comunicazione diretta con i figli anche fuori dal contesto scolastico. Eludendo la sorveglianza degli 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 alunni 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 insegnanti, gli alunni potrebbero correre gli stessi rischi a scuola anche con l'utilizzo dei pc del laboratorio informatico e con un accesso non controllato a internet.

Azioni
Le azioni previste di prevenzione nell'utilizzo delle TIC sono le seguenti:

- **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 (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 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 supervisionato dal personale addetto al centralino, che prima di passare la telefonata si accerta dell'identità dell'interlocutore;**
- **Consentire l'utilizzo del cellulare solo 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, utilizzando software che possono bloccare l'accesso ai siti internet semplicemente esaminando le varie richieste di connessione provenienti dai client collegati in rete locale, in modo tale che anche indipendentemente dal browser in uso su ciascuna macchina, il software sia capace di intercettare le richieste di collegamento e rigettare quelle che non rispettano le regole imposte dall'amministratore.**

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: 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/a viene infastidito/a od offeso/o, suggerirgli/le 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 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.**

APPROVATO DAL CONSIGLIO DI ISTITUTO IL 07/09/2017

UTILIZZO DISPOSITIVI PERSONALI

1. Sono ammessi in classe i seguenti dispositivi digitali mobili (d'ora in avanti semplicemente "dispositivi"): PC portatili, tablet, smartphone ed e-reader.
2. I dispositivi devono essere usati a scuola solo per scopi didattici. L'uso dei dispositivi è pertanto consentito, ma unicamente su indicazione del docente, con esclusiva finalità didattica, in momenti ben definiti e con modalità prescritte dall'insegnante. Durante le ore di lezione, il dispositivo dovrà restare spento e potrà essere acceso solo su autorizzazione del docente. L'utilizzo del dispositivo per scopi non didattici è severamente vietato e sarà oggetto di provvedimenti disciplinari.
3. Gli studenti non possono utilizzare i dispositivi di altri allievi. Ogni utente è responsabile della custodia del proprio dispositivo sia nei locali della scuola sia in ambienti ad essa esterni, le apparecchiature non devono essere mai lasciate incustodite. In particolare egli deve applicare al pc portatile/tablet le regole di utilizzo previste per i pc connessi in rete.
4. Durante le verifiche, è vietato utilizzare il proprio dispositivo, salvo espressa autorizzazione da parte del docente.
5. E' vietato registrare le lezioni e realizzare filmati o foto all'interno dell'Istituto, senza il permesso dell'insegnante e senza il consenso delle persone che vengono riprese. L'utilizzo del dispositivo per la realizzazione di foto e video, se non autorizzato, è severamente vietato e punibile con provvedimenti disciplinari della sospensione da giorni 5 a 15 salvo che il fatto non costituisca reato e quindi si applica la sanzione disciplinare della sospensione superiore a giorni 15 come previsto dal regolamento d'Istituto. In caso di uso improprio, lo studente è obbligato a spegnere il dispositivo.
6. E' vietato utilizzare i dispositivi per compiere atti di prevaricazione, nei confronti di uno studente, e/o del personale docente e ATA, con l'obiettivo di denigrarlo, ridicolizzarlo ed emarginarlo (cyberbullismo).

7. Agli studenti è richiesto di caricare completamente il dispositivo a casa. E' vietato ricaricare il dispositivo in classe. E' consentito utilizzare caricabatterie portatili. Gli studenti devono portare il dispositivo debitamente caricato ogni mattina, al fine di permettere il regolare svolgimento delle lezioni.
8. Si consiglia di dotare il dispositivo di un elemento di riconoscimento personale, che riporti il nome e cognome dello studente, la classe frequentata ed un recapito telefonico.
9. Le famiglie sono invitate a collaborare con l'Istituto, nello spirito della corresponsabilità educativa, evitando, durante l'orario scolastico, di inviare messaggi o effettuare chiamate sui dispositivi degli studenti.
10. Lo studente è tenuto a segnalare tempestivamente al docente eventuali disfunzioni o furti.
In caso di danni causati dagli studenti ad un dispositivo, il costo della riparazione o dell'acquisto sarà addebitato allo studente responsabile e ai suoi genitori.
11. Lo studente è responsabile, a norma delle leggi vigenti, per l'uso improprio del dispositivo e per eventuali danni causati ai dispositivi degli altri studenti.

REGOLAMENTO CYBERBULLISMO

Questo regolamento è da intendersi come parte integrante della e safety e del Regolamento di Istituto

PREMESSA

La scuola rappresenta il luogo in cui gli studenti quotidianamente sperimentano i processi di apprendimento vivendo straordinarie opportunità di crescita intellettuale, di maturazione, di acquisizione di consapevolezza critica e di responsabilità ma, al tempo stesso, in cui si misurano anche con le difficoltà, la fatica, gli errori, le relazioni con pari e i momentanei insuccessi.
Obiettivo di questo regolamento è quello di orientare la nostra scuola nell'individuazione, prevenzione e recupero dei comportamenti deviati, troppo spesso ignorati o minimizzati.
Il fenomeno del cyber-bullismo è così definito dalla Legge 29 maggio 2017, n.71: *"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on-line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo"*. Quest'ultima forma di bullismo, esercitata a distanza attraverso strumenti informatici, si traduce in numerose forme di aggressione e molestie, sovente accompagnate dall'anonimato ed accresciute dal fatto che la distanza del persecutore rispetto alla vittima rende più difficile la percezione della sua sofferenza.

ll bullismo e il cyberbullismo devono essere conosciuti e combattuti da tutti in tutte le forme, così come previsto:
· dagli artt. 3-33-34 della Costituzione Italiana;
· dalla Direttiva MIUR n.16 del 5 febbraio 2007 recante "Linee di indirizzo generali e azioni a livello nazionale per la prevenzione e la lotta al bullismo";
· dalla direttiva MPI n. 30 del 15 marzo 2007 recante "Linee di indirizzo ed indicazioni in materia di utilizzo di 'telefoni cellulari' e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, dovere di vigilanza e di corresponsabilità dei genitori e dei docenti";
· dalla direttiva MPI n. 104 del 30 novembre 2007 recante "Linee di indirizzo e chiarimenti interpretativi ed applicativi in ordine alla normativa vigente posta a tutela della privacy con particolare riferimento all'utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire e/o divulgare immagini, filmati o registrazioni vocali";
· dalla direttiva MIUR n.1455/06;
· LINEE DI ORIENTAMENTO MIUR, aprile 2015, per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo.
· dal D.P.R. 249/98 e 235/2007 recante "Statuto delle studentesse e degli studenti";
· dalle linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo, MIUR aprile 2015;
· dagli artt. 581-582-594-595-610-612-635 del Codice Penale;
· dagli artt. 2043-2047-2048 Codice Civile; · dalla legge 29 maggio 2017, n. 71
· Nuove LINEE DI ORIENTAMENTO MIUR, Ottobre 2017, per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo

Allo scopo di prevenire i citati comportamenti:

Sulla base delle più recenti disposizioni di legge è stato individuato un REFERENTE DEL BULLISMO E CYBERBULLISMO CHE:

- Accoglie segnalazioni di disagio da parte di studenti, docenti e genitori;
- Promuove la conoscenza e la consapevolezza del bullismo e del cyberbullismo attraverso progetti d'Istituto che coinvolgano studenti, genitori e tutto il personale;
- Coordina le attività di prevenzione ed informazione sulle sanzioni previste e sulle responsabilità di natura civile e penale;
- Si rivolge anche a partner esterni alla scuola per realizzare incontri e progetti di prevenzione.

MANCANZE DISCIPLINARI

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, ecc, 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.

• Litigi on line nei quali si fa uso di un linguaggio violento e volgare.

• Registrazione di confidenze raccolte all'interno di un ambiente privato creando un clima di fiducia e poi inserite integralmente in un blog pubblico.

• Molestie attuate attraverso l'invio ripetuto di linguaggi offensivi.

• Ulteriori comportamenti rientranti nelle fattispecie previste dalla Legge 71/2017.

L'INTERVENTO IN CASI DI CYBERBULLISMO: MISURE CORRETTIVE E SANZIONI

La scuola adotta sanzioni disciplinari che possono variare, a seconda della gravità dei fatti accertati, da attività a vantaggio della comunità scolastica fino alla sospensione dalle attività didattiche.

Tali sanzioni devono apparire come le conseguenze dell'atto di cyberbullismo e riflettere la gravità del fatto, in modo da dimostrare a tutti (studenti e genitori) che il cyberbullismo non è in nessun caso accettato. Il provvedimento disciplinare, dovrà tendere alla rieducazione ed al recupero dello studente.

Il cyberbullo – che spesso non è del tutto consapevole della sofferenza provocata – dovrebbe essere aiutato a comprendere la conseguenza del suo gesto nei confronti della vittima mediante la condivisione del dolore e la riflessione sulla condotta sbagliata messa in atto.

Il Consiglio di classe potrà deliberare per i casi più gravi la sospensione fino a 15 giorni, e/o una sanzione disciplinare alternativa (ad es. esclusione dalla partecipazione ad attività ricreative e/o a uscite didattiche e/o viaggi di istruzione; attività a vantaggio della comunità scolastica; produzione di un elaborato scritto, occasione di riflessione sull'infrazione stessa).

La sospensione oltre i 15 giorni sarà disposta dal Dirigente scolastico e il Consiglio di Istituto. Si procederà inoltre alla denuncia alle Autorità competenti e all'attivazione di percorsi per il recupero e il reintegro nella comunità scolastica e sociale.

PROCEDURA SCOLASTICA IN CASO DI ATTI DI CYBERBULLISMO

1) Segnalazione da parte della vittima a genitori e Coordinatore/insegnante
2) Segnalazione al referente del cyber- bullismo e al Dirigente Scolastico
3) Indagine - Verifica e Valutazione di quanto accaduto

Interventi:

a. Supporto alla vittima e comunicazione alla famiglia (convocazione) e supporto nell'affrontare la situazione segnalata, concordando modalità di soluzione e analizzando le risorse disponibili dentro e fuori della scuola

b. Comunicazione ai genitori del cyberbullo (convocazione con lettera disciplinare da inserire nel fascicolo personale)
c. Discussione in classe
d. Valutazione del tipo di provvedimento disciplinare, secondo la gravità:
· imposizione al cyberbullo di svolgimento di azioni positive, per es. lettera di scuse a vittima e famiglia; attività a vantaggio della comunità scolastica;
· esclusione dalla partecipazione a gare sportive e/o a uscite didattiche e/o viaggi di istruzione e/o attività extracurricolari · sospensione dalle attività didattiche da un giorno
· eventuale avvio della procedura giudiziaria: denuncia ad un organo di polizia o all'autorità giudiziaria

Nel caso la famiglia del cyberbullo non collabori, giustifichi, mostri atteggiamenti oppositivi o comunque inadeguatezza, debolezza educativa o sia recidiva nei comportamenti si potrà fare una segnalazione ai Servizi Sociali del Comune.

INFRAZIONI E SANZIONI

Le violazioni alle prescrizioni e ai divieti previsti dal Regolamento, dalle circolari o impartite dai Docenti, sono sanzionate secondo la tabella seguente.

Infrazioni	Sanzioni	Autorità competente	Impugnazioni
Utilizzo del dispositivo e delle sue applicazioni per scopi non didattici in orario scolastico	Nota sul registro	Docente, anche di classe diversa Dirigente scolastico	Organo di garanzia dell'Istituto
Utilizzo del dispositivo per scopi non didattici in orario scolastico che comporta lesione alla morale, alle religioni, all'immagine dell'Istituto, alla dignità delle altre persone, violazione della privacy ecc.	Nota sul registro Ammonizione scritta Sospensione dalle lezioni in base alla gravità dell'infrazione e alla sua reiterazione Denuncia all'autorità competente	Per la nota, ogni docente Per l'ammonizione, il Coordinatore di classe Per la sospensione, il Consiglio di classe o il Consiglio d'Istituto Dirigente scolastico	Organo di garanzia dell'Istituto
Realizzazione di foto e video personali durante l'attività scolastica senza l'autorizzazione del docente e degli interessati	Nota sul registro Ammonizione scritta Sospensione dalle lezioni in base alla gravità dell'infrazione e alla sua reiterazione Denuncia all'autorità competente	Per la nota, ogni docente Per l'ammonizione, il Coordinatore di classe Per la sospensione, il Consiglio di classe o il Consiglio d'Istituto Dirigente scolastico	Organo di garanzia dell'Istituto
Pubblicazione di foto e video personali riferiti all'ambiente scolastico, senza autorizzazione dei docenti e degli interessati	Nota sul registro Ammonizione scritta Sospensione dalle lezioni in base alla gravità dell'infrazione e alla sua reiterazione	Per la nota, ogni docente Per l'ammonizione, il Coordinatore di classe	Organo di garanzia dell'Istituto

	Denuncia all'autorità competente	Per la sospensione, il Consiglio di classe o il Consiglio d'Istituto Dirigente scolastico	
Furto o danneggiamento doloso o colposo al dispositivo di un altro studente	Nota sul registro Ammonizione scritta Sospensione dalle lezioni in base alla gravità dell'infrazione e alla sua reiterazione Risarcimento dei danni (somma necessaria per la riparazione o la sostituzione del dispositivo) Denuncia all'autorità competente	Per la nota, ogni docente Per l'ammonizione, il Coordinatore di classe Per la sospensione, il Consiglio di classe o il Consiglio d'Istituto Dirigente scolastico	Organo di garanzia dell'Istituto
Atti di prevaricazione volontaria e ripetuta nel tempo, compiuti mediante i dispositivi, nei confronti di uno studente, di un docente o del personale ata, con l'obiettivo di denigrarlo, ridicolizzarlo ed emarginarlo (cyberbullismo)	Nota sul registro Ammonizione scritta Sospensione dalle lezioni in base alla gravità dell'infrazione e alla sua reiterazione Risarcimento dei danni (somma necessaria per la riparazione o la sostituzione del dispositivo) Denuncia all'autorità competente	Per la nota, ogni docente Per l'ammonizione, il Coordinatore di classe Per la sospensione, il Consiglio di classe o il Consiglio d'Istituto Dirigente scolastico	Organo di garanzia dell'Istituto

Approvato dal c.d.i. il 26 settembre 2019