FUTURA LA SCUOLA PER L'ITALIA DI DOMANI

Ministero dell'Istruzione e del Merito

ISTITUTO STATALE COMPRENSIVO "Angelo Battelli"
Scuola Secondaria di 1° grado ad indirizzo musicale
Via della Maternità n. 46 - 47863 NOVAFELTRIA (RN) – Telefono 0541/920068 - 846520
Cod. Mecc. RNIC811008 – C.F. 80008010417 – C.U.U. UFQWDK
Sito www.icbattelli.edu.it – E-mail rnic811008@istruzione.it / rnic811008@pec.istruzione.it

Alla cortese attenzione di tutti i Docenti
personale ATA

p.c. DSGA

p.c. DPO
Ing. ……

Oggetto: Regolamento e indicazioni per la Sicurezza Informatica

Fonti normative

- D Lgs.196/2003.
- Piano Nazionale Scuola Digitale, pilastro fondamentale de La Buona Scuola (legge 107/2015).
- Regolamento generale per la protezione dei dati (Regolamento UE 2016/679 del 27 aprile 2016).
- Codice comportamentale MIUR 28/11/2016.
- Linee di orientamento per la prevenzione e il contrasto del cyber bullismo nelle scuole (art. 4 L. 71/2017).
- Dichiarazione dei Diritti in Internet – Testo legislativo (L. 71/2017 ; Nota MIUR Prot.5515 del 27/10/2017).
- Linee di orientamento prevenzione e contrasto – Bullismo e Cyberbullismo-MIUR.
- Codice Penale e Civile in materia di cybercrimine e tutela della privacy.

L'istituto Angelo Battelli di Novafeltria fornisce a ogni utente: docente, alunno e personale ATA una mail d'istituto. Da non confondere con la mail Istruzione.
La mail d'istituto è creata attraverso il Dominio Valmar con le Google Workspace ed è così strutturata

nome.cognome@battelli.istruzioneer.it

Con l'account viene fornita una password temporanea che dovrà essere modificata al primo accesso e ricordata dall'utente, ma mai memorizzata sui computer della scuola.
Un eventuale Reset (cambiamento) della password potrà essere effettuato solo dall' Animatore Digitale; nell'eventualità si chiede di fare riferimento ai coordinatori di classe o di plesso, **ma non rivolgersi alla segreteria**.
La mail permette a tutti gli utenti di accedere alla piattaforma Google Workspace e fruire dei servizi rispettando le seguenti.

Ai sensi del Regolamento UE 2016/679 e del Decreto Legislativo 30 giugno 2003, n. 196, dichiarano di ricevere l'informativa sulle seguenti condizioni d'uso della piattaforma dedicata Valmar.
Ogni alunno riceve un account con nome utente e password per l'accesso alle applicazioni di Google durante le attività didattiche.
I dati di accesso consentono:

- la creazione, la condivisione e l'uso di files salvati in rete durante le attività didattiche
- le comunicazioni fra gli utenti iscritti nello stesso dominio (valmar.istruzioneer.it)
- l'uso delle applicazioni contenute nei dispositivi in dotazione alla classe
- l'uso delle stesse applicazioni a casa con altri dispositivi personali.

L'uso dei dispositivi in classe:

- la scuola primaria ha in dotazione pc, notebook; ognuno può essere utilizzato da qualsiasi alunno con il proprio account personale
- gli alunni devono prestare la dovuta attenzione per non danneggiare i dispositivi durante le attività in classe

L'uso delle applicazioni con altri dispositivi a casa:

1. ogni alunno può accedere ai propri files o a quelli condivisi con il proprio gruppo anche da casa su PC, tablet, smartphone o altri dispositivi;

2. ogni alunno può comunicare e condividere files solo con gli altri utenti che appartengono all'organizzazione scolastica "valmar";
3. tutti i contenuti condivisi in rete dagli alunni sono controllati dagli amministratori dell'organizzazione e devono essere attinenti alle attività didattiche da svolgere.

Dopo la fine del percorso scolastico dell'alunno l'account sarà ancora utilizzabile per 180 giorni.
L'alunno potrà scaricare i files che ritiene utili da conservare sui propri dispositivi personali.
Dopo 180 giorni l'account sarà disattivato, ma il contenuto sarà ancora conservato nel dominio.
Alla fine dell'ultimo periodo anche il contenuto sarà eliminato.

La violazione di queste norme determinerà la rimozione temporanea o permanente dell' account.

A tutela della privacy, l'indirizzo di posta elettronica del minore non verrà divulgato in alcun contesto in accordo al trattamento dei dati personali di cui alla normativa vigente sopra richiamata.

Si precisa che il servizio offerto non tratta dati sensibili, ovvero dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

REGOLAMENTO GENERALE PER UN USO CORRETTO E CONSAPEVOLE DELLE ATTREZZATURE INFORMATICHE, MULTIMEDIALI E DELLA RETE.

CONSIDERAZIONI GENERALI

Le nuove tecnologie informatiche rappresentano per la scuola un importante strumento per rinnovare ed ampliare le possibilità didattiche, per facilitare l'apprendimento e l'integrazione di tutti gli alunni.
Il nostro istituto ha investito e investe consistenti risorse economiche per incrementare l'uso di queste tecnologie per favorire lo sviluppo di idee e progetti, per conseguire competenze e abilità specifiche e trasversali, per l'aggiornamento, per facilitare il lavoro quotidiano degli operatori della scuola e per condividere e diffondere informazioni e conoscenze, come nel caso del sito web dell'istituto.
Le nuove tecnologie costituiscono però anche una potenziale fonte di rischi; infatti come da comunicazione del Ministero dell'Istruzione e del

Merito si rende noto che "Stiamo rilevando il blocco di mail di phishing indirizzate al personale ministeriale da parte dei sistemi di sicurezza del M.I.; tali messaggi sono indirizzati a caselle di posta elettronica istituzionali, provenendo da mittenti verosimili e rispetto ai quali nei testi si richiedono azioni di accesso a pagine web/download file che in realtà possono recare problemi alla postazione di lavoro e, a cascata, all'infrastruttura tecnologica del M.I. con la stessa frequenza inoltre si rileva anche attività anomala da parte di alcune caselle di posta istituzionali che inviano mail di spam all'insaputa dell'utente titolare dell'account, la cui compromissione il più delle volte è dovuta ad infezioni da virus sulle postazioni di lavoro o sui dispositivi utilizzati per l'accesso.
La causa delle suddette situazioni risiede sicuramente in un'intensa e sempre più sofisticata attività da parte dei cyber attaccanti in internet, interessati a carpire informazioni riservate sensibili, personali e/o dell'Organizzazione, ma anche soprattutto in comportamenti da parte delle persone non sempre in linea con le buone prassi di sicurezza e le indicazioni in tal senso da parte dell'Amministrazione".
Il nostro Istituto intende promuovere l'educazione dei propri alunni ad un uso consapevole, positivo e responsabile delle tecnologie e della multimedialità. Considerato anche l'impegno finanziario che la scuola deve sostenere per l'acquisto e la manutenzione di tali strumenti, si impone la necessità di procedere ad una regolamentazione del loro uso, per permetterne un utilizzo diffuso, ma anche consapevole, responsabile e critico.
Le attrezzature informatiche costituiscono un patrimonio della scuola e vanno utilizzate con diligenza e nel rispetto di tutti gli utenti, con il presente regolamento se ne disciplinano le modalità di utilizzo.
Il Dirigente Scolastico in collaborazione con il Team Digitale, ha elaborato il seguente documento per l'uso consapevole delle tecnologie con riferimento alle linee guida delle politiche nazionali del Ministero dell'Istruzione e del Merito.

Il presente documento, parte integrante del Regolamento di Istituto, sarà portato a conoscenza dei genitori, degli allievi e di tutto il personale della scuola.

ARTICOLAZIONE DEL REGOLAMENTO

1. TEAM DIGITALE

Il Team Digitale è composto da tre docenti, uno per ogni ordine di scuola, coordinati dall'Animatore Digitale. Il Team e l'animatore si rinnovano per legge ogni tre anni. Il team si avvale della collaborazione del Pronto Soccorso tecnico, garantito dall'assistente amministrativa.
L'istituto si avvale anche della consulenza di un tecnico informatico dell'Ambito 21.
La commissione si occupa della promozione dell'innovazione scolastica prevista dalla normativa, come sopra richiamata, condivisione e gestione problematiche connesse ai sistemi informatici, valorizzazione delle nuove didattiche digitali.
A tale scopo vengono organizzati corsi di formazione, caffè digitali, incontri con formatori esterni. Il team è coinvolto nella predisposizione nella progettazione e attuazione dei PON, PNRR, Next generation classroom.

Membri della commissione e/o responsabili anno scolastico 2023/2024

Nome	Ruolo	Ordine di Scuola	
Katia Piastra	Animatore Digitale	Primaria	
Tatiana Cannone	Team Digitale	Infanzia	
Patrizia Merli	Team Digitale	Primaria	
Lara Tosi	Team Digitale	Secondaria di Primo Grado	
Patrizia Paolacci	Pronto Soccorso Tecnico	ATA	

Antonio Di Terlizzi	Tecnico Informatico		Ambito 21

Il Team nell'istituto ha i seguenti compiti:
- divulgazione del Piano Nazionale Scuola Digitale;
- attuare raccordo con i referenti di informatica di plesso e supporto informatico ai docenti anche su problematiche connesse ai registri on line;
- gestire i laboratori di informatica del proprio plesso;
- tenere incontri periodici con D.S.;
- progettare e sviluppare percorsi finalizzati all'utilizzo delle nuove tecnologie;
- collaborazione con il docente di tecnologia che si occupa del Sito della scuola;
- gestire il sito MIRROR;
- partecipare a corsi di aggiornamento specifici;
- proporre corsi di formazione per alunni e docenti;
- elaborare una verifica e valutazione finale, e fare nuove proposte;
- supportare la Dirigenza per la partecipazione a bandi PON, PNRR
- supporto ai docenti;
-raccolta dei bisogni formativi tecnologici degli insegnanti e problematiche connesse.

Compito del team è l'attuazione del PNSD, ora Futura Scuola per l'Italia di Domani, coerentemente con quanto individuato nel PTOF dell'istituto.

2. DISPOSITIVI MULTIMEDIALI CUI SI APPLICA IL REGOLAMENTO

Sono oggetto del regolamento tutti i dispositivi elettronici presenti a scuola e la rete, sia cablata che wireless.
I dispositivi elettronici comprendono: PC, monitor, tastiere, mouse, cavi, tablet-ipad, stampanti, LIM, proiettori, scanner, fax, apparecchiature wireless, macchine fotografiche e videocamere ecc.

3. STRATEGIE DELL'I.C. PER GARANTIRE LA SICUREZZA DELLE TECNOLOGIE

1. Il personale scolastico accede alla rete della scuola tramite un codice di credenziali dato dalla segreteria che va inserito in SSID- HOTSPOT Battelli
2. Separazione della rete didattica dalla rete amministrativa.
3. Utilizzo di firewall per impedire l'accesso dall'esterno ai computer dell'Istituto.
4. Filtrare l'accesso a siti non appropriati.
5. L'utilizzo dei laboratori/carrelli mobili è regolamentato; gli alunni possono accedere o usufruirne solo in presenza di docenti.
6. L'utilizzo dei dispositivi in classe e la connessione a Internet avviene sotto il controllo del docente; la connessione a Internet da parte degli alunni, se non autorizzati dagli insegnanti, è vietata.
7. L'insegnante è responsabile dell'utilizzo di internet da parte degli alunni nelle proprie ore di lezione.
8. Il sistema informatico dell'Istituto viene regolarmente controllato, per prevenire ed eventualmente rimediare a possibili disfunzioni dell'hardware e/o del software.
9. Il sistema informatico della scuola è provvisto di un software antivirus aggiornato periodicamente.
Si chiede di scansionare periodicamente per la ricerca virus le postazioni e i dispositivi di lavoro utilizzati.
Nel caso di utilizzo del PC personale (telelavoro/smart working) assicurarsi periodicamente:

- che il sistema operativo sia aggiornato;
- che la propria postazione di lavoro sia dotata di antivirus e che questo sia aggiornato per una periodica scansione;
- che le proprie password di posta e strumenti di lavoro siano sicure, ovvero complesse, non facilmente individuabili, diverse per servizi distinti e che, al momento della modifica, non siano apportate solo piccole variazioni (come ad esempio numerazioni progressive,...).

10. I supporti di archiviazione dati di docenti e alunni devono essere preventivamente scansionati con antivirus. Si consiglia di utilizzare il drive e la condivisione.
11. I software utilizzabili sono solamente quelli autorizzati dalla scuola, regolarmente licenziati e/o open source riconosciuti secondo la vigente normativa.
12. È vietato modificare le impostazioni tecniche dei singoli computer, installare programmi senza preventivamente aver chiesto il permesso e consultato il responsabile digitale.
13. L'Istituto riferisce alle autorità competenti se è stato trovato materiale illegale.

4. LINEE GUIDA PER I DOCENTI
a) UTILIZZO DI INTERNET

Il personale può accedere a Internet per motivi di lavoro e per le attività connesse alla funzione docente.
Nell'uso di internet e della posta elettronica non sono consentite le seguenti attività:
1. Scaricare (download) software e file non necessari all'attività istituzionale;
2. Farne un uso che possa in qualche modo recare qualsiasi danno all'Istituto o a terzi.
3. Immettere in rete foto o filmati non autorizzati
4. Scaricare file che potrebbero essere protetti da diritti d'autore.
5. Non lasciare il pc portatile incustodito.
6. Non installare software sulle proprie postazioni di lavoro soprattutto se a seguito di sollecitazioni via email.

Qualora si dovesse incorrere in messaggi mail di phishing si ricorda quanto segue:
- non dare seguito all'apertura di file non attesi, dalla dubbia provenienza o che giungano da caselle non note. Nel caso provengano da personale tecnico dell'Amministrazione verificare attentamente il contesto (la mail attesa? Le frasi sono scritte con grammatica corretta? Il software da installare ha un fine specifico? Eventuali link dell'email rimandano a siti attendibili? Il mittente è corretto?).

In ogni caso l'utente è direttamente responsabile dell'uso del servizio di accesso ad Internet, dei siti ai quali accede, delle informazioni che immette e riceve.

b) UTILIZZO DI DISPOSITIVI, MACCHINE E SOFTWARE

1. Non usare l'account di lavoro per registrarsi in internet per fini non riconducibili alla sfera di lavoro ed evitare di salvare le password nel browser di navigazione internet.
2. Non è consentito lasciare account personali attivi sui dispositivi della scuola
3. Tutti i file contenenti dati sensibili vanno cancellati e non salvati sui dispositivi
4. Non è consentito l'uso di software/programmi di dubbia provenienza e di cui non si conosce la validità didattica. Qualora si abbia la necessità di utilizzare un software diverso da quello installato rivolgersi al Team digitale che insieme alla Dirigente valuterà l'opportunità della richiesta.
5. È vietato inserire password alle risorse informatiche assegnate (es. password che non consentano l'uso del pc agli amministratori di sistema)

c) GESTIONE DEL MATERIALE INFORMATICO

Durante le sessioni di lavoro ogni utente (docente, studente, operatore della scuola) è responsabile dell'attrezzatura che gli viene messa a disposizione e risponde di eventuali danni arrecati.
Ogni plesso si organizza in modo autonomo, e il referente di plesso farà riferimento al team digitale per le modalità di gestione pratica delle macchine.
Ogni anomalia deve essere segnalata immediatamente sia a voce che per iscritto al responsabile di plesso e al Team Digitale e al Dirigente.
d) OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY
È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di designazione di incaricato del trattamento dei dati ai sensi del **GDPR 679/2016** (Regolamento Europeo per la protezione dei dati personali).

5. LINEE GUIDA PER PERSONALE ATA
Per il personale ATA valgono le stesse indicazioni prescritte per i docenti.

6. LINEE GUIDA PER GLI ALUNNI

a) USO DEI DISPOSITIVI ELETTRONICI: ALUNNI H/DSA/BES:
Durante le lezioni gli alunni possono utilizzare i dispositivi della scuola (computer, tablet) connessi alla rete internet con le relative disposizione

d’istituto; il docente di classe o di sostegno deve vigilare sulla correttezza dell’utilizzo (ad esempio che l’alunno non utilizzi materiale non consentito). assicurandosi precedentemente che il dispositivo sia funzionante e pronto all'uso.
Nel caso del laboratorio mobile o dell’aula di tecnologia sarebbe opportuno predisporre un registro per il prestito per verificare da chi è stato preso il materiale e da chi va riconsegnato.
b) USO DELLE CHIAVETTE USB
Si chiede di evitare l’utilizzo delle chiavette personali vista le ripetute segnalazione di virus trasmessi nei sistemi informatici della scuola, si consiglia l’utilizzo del Drive e la condivisione sul dominio Battelli.
c) USO DEL CELLULARE A SCUOLA
Per quanto riguarda l’utilizzo dei cellulari si rimanda alle indicazioni contenute nella circolare della Dirigente n. 10 del 25/09/2023 Che verrà allegato al presente documento.

7 PRIVACY

a) USO DEI SOCIAL NETWORK
I social media sono dei siti appositi di tipo 2.0 nei quali gli utenti possono condividere contenuti di vario tipo. Tra i più diffusi per ora citiamo Facebook, Twitter, Messenger, Whatsapp, Flickr, Youtube,Instagram e altri.

1. L’uso dei social media, utilizzando apparecchiature della scuola, deve essere fatto solo per motivi professionali.
2. L’amicizia tra alunni e insegnanti sui social media è vivamente sconsigliata per le implicazioni sociali e di privacy correlate.
3. Il canale di comunicazione ufficiale tra scuola e famiglia è il Registro Elettronico.
4. Nell’uso dei social media, particolare attenzione deve essere prestata ai commenti e ai post relativi all'ambiente scolastico da parte di alunni e adulti (docenti, genitori, personale scolastico ed educativo in generale).
Riflessioni, considerazioni e commenti del personale della scuola, docenti e non, non devono ledere il diritto alla riservatezza degli alunni, anche a loro indirettamente riconducibili e non devono ledere l’immagine dell’Istituzione scolastica che rappresentano.

L'uso dei social media deve avvenire nel rispetto della normativa vigente sulla privacy e la diffamazione.
Si ricorda inoltre la nuova circolare in materiale Ministeriale sui dipendenti della Pubblica amministrazione. Si rimanda anche qui alla circolare della Dirigente Piano D'istituto della Comunicazione e Legge sul RIFERIMENTI

b) FOTOGRAFIE, RIPRESE AUDIO E VIDEO A SCUOLA
Le immagini e i filmati costituiscono dati personali o fonti di rinvenimento di dati personali.
1. La scuola può realizzare foto/riprese per attività istituzionali e deve provvedere alla loro conservazione per il tempo necessario al loro utilizzo e per i soli fini strettamente necessari alle finalità istituzionali.
2. Se la scuola intende utilizzare i filmati per la partecipazione a mostre, fiere, concorsi, deve raccogliere il consenso espresso e specifico della famiglia.
3. Nel caso in cui la scuola, nel corso di un partenariato con soggetti esterni, gestisca eventi o manifestazioni, le cui rappresentazioni fotografiche verranno usate per comunicare l'evento a mezzo stampa o televisione, la scuola può esclusivamente mettere in contatto il soggetto esterno con le famiglie per la gestione di richiesta del consenso, nella quale sia chiaro l'uso che si vuole fare della ripresa.
4. Le riprese fotografiche/video a scuola da parte di esterni non sono consentite. Nel caso di operatori esterni, fotografi, (anche genitori che riprendono per tutti) che effettuano riprese degli alunni al fine di documentare un certo evento (l'inizio dell'anno scolastico, la recita, la manifestazione sportiva ecc.), deve essere comunicato il nominativo al Dirigente perché possa verificare le credenziali del fotografo. La scuola mette lo stesso in contatto con le famiglie che decideranno se prestare il loro consenso alla realizzazione fotografica.
5. Le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici dei propri figli non violano la privacy se sono fatte a fini personali e destinate ad un ambiente scolastico, per cui il loro uso è legittimo. Non possono essere pubblicate e diffuse in rete, anche sui social network. In caso di pubblicazione è necessario informare adeguatamente le persone coinvolte nella registrazione e ottenere l'esplicito consenso.
Le fotografie sono consentite solo per scopo didattico e per documentare esperienze didattiche cercando di evitare di ledere la Privacy degli alunni. Si consiglia di oscurare il volto degli alunni.
Le eventuali foto e video non vanno conservati nei dispositivi personali dei docenti, ma in pendrive (memoria USB) e poi eliminati dopo il loro utilizzo.

c) COPYRIGHT E USO DELLE RISORSE IN RETE

La legge tutela la proprietà intellettuale tramite il copyright. I materiali reperiti in rete ed utilizzati dagli alunni o dagli insegnanti devono essere di libero utilizzo.

1. Foto: le foto utilizzate non devono essere coperte da copyright e deve essere citata la provenienza dei materiali utilizzato. Si suggerisce di cercare foto di libero utilizzo o libera modifica inserendo questi parametri nei filtri di ricerca.
2. Musica: le musiche inserite nei filmati devono essere di libero utilizzo, se coperte da diritti SIAE questi devono essere pagati. Musiche di libero utilizzo sono disponibili in "JAMENDO".
3. Non si possono scaricare film in modo illegale e neppure utilizzare materiale scaricato illegalmente dalla rete.

d) SOFTWARE UTILIZZABILI A SCUOLA

Così come la musica, le immagini o le parole, anche il software è tutelato come prodotto dell'ingegno, quindi sottoposto a copyright. Quindi possono essere utilizzati:

1. software proprietari, legalmente acquistati, come i sistemi operativi Windows o Mac, oppure programmi come Microsoft Office, Antivirus ecc dalla scuola.
2. software open source e free, come il sistema operativo Linux e le sue derivate, oppure programmi come Libre Office, Geogebra, Free plane, The Gimp, ecc.

Il nostro istituto ha da anni scelto di utilizzare software free ogni volta che è possibile e comunque le installazioni non vanno effettuate dai singoli docenti, ma richieste al Team digitale e autorizzate dal Dirigente Scolastico e poi installate dal personale addetto.

8 USO DELLE RISORSE HARDWARE E SOFTWARE

a) Modalità di utilizzo delle risorse hardware e software

1. Chi accede alle risorse informatiche dell'Istituto Comprensivo è tenuto a trattare con il dovuto riguardo le apparecchiature e i materiali di cui si serve.
2. Non si consumano bevande e/o cibi durante il lavoro informatico.
3. Non si possono installare programmi. Le installazioni possono essere effettuate solo dai membri della Commissione Informatica.
4. Non si possono spostare apparecchiature, connessioni con le periferiche, etc.

5. Non si possono copiare software presenti sulle macchine dell'Istituto.
Nell'utilizzo delle risorse informatiche sono inoltre vietate:
1. attività commerciali;
2. tutte le attività che possono rappresentare una violazione della legge in materia di Copyright, fra le quali la copia non autorizzata di software brevettato;
3. tutte le attività che compromettono in qualsiasi modo la sicurezza delle risorse;
4. ogni altra attività illegale qui non elencata.
b) Uso delle stampanti
1. Se sono necessarie molte copie di un documento si invitano i docenti a ricorrere alle fotocopie.
2. Se si stampano immagini da internet, evitare la stampa di intere pagine web comprese di immagini a colori, loghi, banners pubblicitari, ecc...ma salvare in formato testo (.txt) e stampare il contenuto.
In ogni caso cercare di limitare allo stretto indispensabile l'uso della stampante.

Allegati:
1- Vademecum sicurezza informatica
2- Regolamento E-policy