



FUTURA

**LA SCUOLA
PER L'ITALIA DI DOMANI**



ISTITUTO COMPRENSIVO STATALE C.T. BELLINI - NOVARA

Via Vallauri, 4 - 28100 Novara

Codice Fiscale: 94062750032 - Codice Meccanografico: NOIC82300L

Tel. 0321 692625 - Sito web: www.istitutocomprensivobellini.edu.it

E-mail: noic82300l@istruzione.it - PEC: noic82300l@pec.istruzione.it

Regolamento di utilizzo rete internet e email istituzionale

Premesso che l'utilizzo degli strumenti di lavoro, nei quali sono compresi anche i sistemi e le risorse informatiche e telematiche, deve sempre ispirarsi al principio della diligenza e correttezza, propri del rapporto di lavoro, l'Istituto adotta il presente regolamento diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati, nonché, originare responsabilità in capo all'Istituto ovvero ai singoli lavoratori.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni fornite a tutti i Soggetti Autorizzati/delegati in attuazione del Regolamento 2016/679/UE (nel seguito "GDPR") e del D. lgs. 30 giugno 2003 n. 196 (di seguito "Codice") come modificato dal D. lgs. 101/2018, relativamente alle prescrizioni non in contrasto con il GDPR, nonché integrano le informazioni fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

Si tiene conto, purché non in contrasto con il GDPR, delle principali prescrizioni e le linee guida del Garante privacy in relazione al trattamento di dati personali effettuato dai datori di lavoro, (provvedimento "Linee-guida per il trattamento di dati dei dipendenti" del 23 novembre 2006) ai fini delle verifiche per il corretto utilizzo della posta elettronica e della rete Internet da parte dei dipendenti (provvedimento del 1° marzo 2007) nonché delle previsioni dell'art. 4 L. 300/70, come modificato dal D.lgs. 151/2015 relativamente ai controlli sugli "strumenti di lavoro", e tenendo presente le indicazioni fornite dal WP 29 con la "Opinion 2/2017 on data processing at work".

Dal contesto tracciato dal Garante nelle premesse dei citati provvedimenti emerge che:

- compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;
 - spetta sempre ai datori di lavoro adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e dei dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità;
 - è necessario tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;
 - l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di file di log, della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta dei file di log di traffico e-mail e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;
 - le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili.
- Tutto ciò premesso l'istituto ha deciso di dotarsi di un regolamento che disciplini l'uso della rete internet e dell'account istituzionale.

l'IC C.T. Bellini (NO) mette a disposizione dei docenti, studenti e personale Ata una mail istituzionale allo scopo di fornire :

- ai propri studenti e ai docenti supporti che agevolino la fruizione dell'attività didattica a distanza e le comunicazioni docenti-studenti-famiglie.

- al personale Ata ulteriore *strumento* per la gestione delle comunicazioni e delle informazioni nell' espletamento del loro servizio sia in presenza che attraverso lo Smart Working

Il presente documento ha ,quindi, l'obiettivo di regolamentare l'utilizzo della posta elettronica per gli utenti di tali servizi nell'ambito della struttura scolastica IC C.T. Bellini (NO).

Le presenti regole di sicurezza si pongono l'obiettivo di fornire agli utenti idonee misure di sicurezza e linee di comportamento adeguate per utilizzare in modo conforme e non rischioso la posta elettronica .

Il Regolamento è adottato in conformità al Provvedimento del Garante per la tutela dei dati personali del 1° marzo 2007(**doc. 1387522**), nella consapevolezza che gli **“account”** di posta aziendale composti da “nome e cognome”, ancorché accompagnati dal dominio aziendale, sono a tutti gli effetti “dati personali” (*ex art 4 del GDPR*) e per questo necessitano della corretta applicazione delle tutele imposte dalla relativa normativa in materia (Reg. UE 2016/679 e Codice Privacy così come modificato dal D.Lgs. 101/2018).

Il servizio è inteso quale strumento di semplificazione, utile in funzione della didattica, della ricerca, dell'amministrazione, dei servizi agli utenti e di altre attività strumentali o correlate ai fini istituzionali dell'Istituto, in adesione alle seguenti norme:

- Codice dell'Amministrazione Digitale, D.Lgs. 7 marzo 2005, n. 82, modificato e integrato dal decreto legislativo 22 agosto 2016 n. 179 e dal decreto legislativo 13 dicembre 2017 n. 217;
- Direttive impartite in materia dal Ministero per la Pubblica Amministrazione e l'Innovazione;
- Codice in materia di protezione dati personali (D.Lgs 196/2003) integrato dal D.Lgs 101/2018
- Regolamento UE 2016/679 (G.D.P.R.).
- Art 4 Statuto dei Lavoratori (L. 20 maggio 1970 nr. 300)

PREMESSA

Nel presente regolamento i termini di seguito elencati hanno il significato ai medesimi associato:

- a) Istituto: Istituto comprensivo C.T. Bellini (NO)”.
- b) Amministratore di sistema: l'amministratore della rete interna dell'Istituto.
- c) Amministratore di posta: l'amministratore del servizio di posta elettronica dell'Istituto.
- d) Servizio: servizio di posta elettronica con casella messa a disposizione dall'Istituto.
- e) Account di posta elettronica: è costituito da username, password ed indirizzo di posta.
- f) Fornitore: ditta che fornisce il servizio di posta elettronica.
- g) Utenti: tutti coloro che hanno accesso al servizio di posta elettronica attuato dal fornitore e messo a disposizione dell'Istituto alla luce del presente regolamento.
- h) Rete: la rete interna dell'Istituto.
- i) Abuso: qualsivoglia violazione del presente regolamento o di altre discipline civili, penali e amministrative che disciplinano le attività e i servizi svolti sulla rete.
- j) dominio: nome.cognome@istitutocomprensivobellini.edu.it

Art. 1 – Posta elettronica

1. La posta elettronica costituisce modalità normale di trasmissione delle comunicazioni ufficiali dell'Istituto, e **sarà utilizzata come strumento di comunicazione al fine di porre in essere un'azione volta ai criteri di economicità, di efficacia e di pubblicità prevista dalla normativa vigente.**

2. Tutto il personale dovrà utilizzare esclusivamente la mail istituzionale come strumento di trasmissione con la scuola

3. Tutte le comunicazioni interne indirizzate ai docenti, circolari, comunicazioni della presidenza, ecc., saranno date utilizzando le suddette caselle di posta elettronica e avranno valore ufficiale di notifica.

4. La casella è strettamente personale e non è ammesso l'utilizzo da parte di persone diverse dall'assegnatario, né questi può cederla a terzi.

5. Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano a non commettere violazioni alle norme generali e speciali civili, penali ed amministrative, nonché al presente regolamento, aderendo ad un principio di autodisciplina.

3. L'indirizzo di posta elettronica può essere correlato ad altri servizi come accesso a portali, piattaforme didattiche (es. Google G suite) e tutti gli ambienti internet legati solo ed esclusivamente ad attività lavorative e didattiche.

Art. 2 – Soggetti che possono avere accesso al servizio di posta elettronica

1. La casella viene assegnata agli utenti che necessitano di tale servizio a scopi lavorativi e/o didattici: docenti a tempo determinato o indeterminato, studenti, personale interno, previa autorizzazione a terze parti e viene ritirata alla cessazione dello stesso.

Art. 3 – Tipologie di caselle

1. L'indirizzo è del tipo nome.cognome@dominio.it

2. Ogni casella di posta elettronica viene fornita insieme ad uno spazio disco limitato.

3. L'amministratore di posta, tenuto conto delle risorse tecniche a disposizione, può limitare momentaneamente il numero di account per categorie di utenti ed incrementarlo con gradualità.

4. L'attivazione dell'account avverrà:

- per gli alunni all'atto dell'iscrizione o successivamente entro il primo anno di iscrizione,
- per i docenti e per il personale Ata contestualmente alla presa di servizio .

Art. 4 – Condizioni di utilizzo

1. Qualsiasi utilizzo della posta elettronica e servizi ad essa collegati viene associato ad un persona fisica cui imputare le attività svolte.

2. L'Utente ottiene l'accesso impegnandosi ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi di posta elettronica comprese le funzionalità ad essa collegate e essersi impegnato a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.

3. L'Utente è responsabile dell'attività espletata tramite il suo account.

4. L'Utente si impegna ad adoperarsi attivamente per salvaguardare la riservatezza della sua password ed a segnalare qualunque situazione che possa inficiarla.

5. L'Utente si impegna a segnalare, con tempestività, all'amministratore di posta eventuali malfunzionamenti della casella di posta a lui assegnata.

6. Di norma gli Utenti possono accedere gratuitamente al servizio, tramite le infrastrutture dell'Istituto.

7. Restano a carico dell'Utente eventuali oneri relativi a collegamenti da punti di accesso privati.

8. L'Utente riconosce che le comunicazioni ufficiali, quali circolari e convocazioni di organi e commissioni, inviate agli indirizzi di posta elettronica valgono quali comunicazioni interne e si considerano consegnate al momento dell'avvenuto regolare invio.

8. Sotto la propria personale responsabilità e per gli alunni minorenni, sotto la responsabilità dei tutori, l'account può essere utilizzato per scopi personali ma a condizione che siano leciti , in questo caso si dovrà aver cura di prelevare e conservare eventuali documenti privati in un cloud o hardware di proprietà, in quanto a fine servizio o a compimento del ciclo scolastico, la casella di posta verrà cancellata definitivamente e non si potrà più recuperare nessun documento o file ivi giacente.

Art. 5 – Obblighi dell'Istituto

1. L'Istituto si impegna a fornire il servizio in modo continuativo, fatte salve eventuali sospensioni dovute all'ordinaria o straordinaria manutenzione, malfunzionamenti e ad altre eventualità.

2. L'Istituto si impegna ad utilizzare i dati, già forniti dall'Utente ai sensi della normativa vigente, con chiaro riferimento al "D.Lgs. 30 giugno 2003, n. 196 (così come modificato dal D.lgs 101/2018) Codice in materia di protezione dei dati personali" e successiva normativa nazionale e comunitaria, con particolare riferimento al Regolamento UE 2016/679 (G.D.P.R.), ai soli fini

dell'erogazione e gestione del servizio e di attuare quanto in suo potere per proteggere la privacy dell'Utente medesimo.

Art. 6 – Limiti di responsabilità dell'Istituto

1. L'Istituto si serve di fornitori che si impegnano ad attuare tutte le misure ritenute necessarie e sufficienti a minimizzare il rischio di perdita d'informazioni; ciò nonostante l'Utente solleva l'Istituto da ogni responsabilità ed obbligazione in relazione alla cancellazione, al danneggiamento, al mancato invio/ricezione o all'omessa conservazione di messaggi di posta (e-mail) o di altri contenuti, derivanti da guasti e/o malfunzionamenti degli apparati di gestione e, in generale, dall'erogazione del servizio stesso.
2. L'Istituto si riserva il diritto di non memorizzare o di cancellare i messaggi dell'Utente stesso, qualora questi ecceda lo spazio disco a sua disposizione.
3. Non sono previste attività di backup e di ripristino individuale sui server che sono gestiti esternamente e internamente.

Art. 7 – Riservatezza della posta elettronica

1. L'Istituto persegue la riservatezza e l'integrità dei messaggi di posta elettronica e servizi ad essa collegati diretti alle caselle personali durante il loro transito e la loro permanenza nel sistema di posta.
2. Per il raggiungimento di tale obiettivo l'Amministratore di Sistema, l'Amministratore di posta ed il Fornitore possono avvalersi anche di strumenti idonei a verificare, mettere in quarantena o cancellare i messaggi che potrebbero compromettere il buon funzionamento del servizio.
3. In linea generale, i messaggi di posta sono conservati nella mailbox associata all'Utente, finché non vengano dallo stesso rimossi.

Art. 8 – Liste di utenti

1. In osservanza di quanto disposto dal D.Lgs. 30 giugno 2003, n. 196 e successiva normativa nazionale e comunitaria, Regolamento UE 2016/679 (G.D.P.R.), al fine di tutelare la riservatezza degli utenti e la libertà e segretezza della corrispondenza, possono essere predisposte liste di utenti, distinte per oggetto, volte a semplificare le comunicazioni istituzionali
2. In particolare, possono essere attivate liste permanenti, in relazione alla qualifica, alla funzione svolta, alla materia di insegnamento, per le comunicazioni istituzionali.
3. Possono inoltre essere attivate liste temporanee in relazione a progetti od esigenze particolari
4. L'utilizzo delle liste è disciplinato dal Dirigente.

Art. 9 – Attività vietate

1. È vietato usare il servizio:
 - a. in modo difforme da quanto previsto nel presente regolamento;
 - b. in modo difforme dalle regolamentazioni dettate dai responsabili della rete e del servizio di posta;
 - c. in modo difforme da quanto previsto dalle norme penali, civili e amministrative generali e specifiche in materia;

Art. 10 – Ulteriori divieti, limiti di utilizzo, responsabilità dell'Utente

1. L'Utente si assume ogni responsabilità penale e civile ed il carico di ogni eventuale onere derivante dall'uso improprio del servizio; esonera contestualmente l'Istituto da ogni pretesa o azione che dovesse essere rivolta all'Istituto medesimo da qualunque soggetto, in conseguenza di tale uso improprio.
2. In nessun caso l'Utente potrà utilizzare la posta elettronica e servizi ad essa collegati per diffondere codici dannosi per i computer quali virus e simili.
3. È assolutamente vietato tentare di accedere in modo non autorizzato, tramite operazioni di pirateria informatica, contraffazione della password o altri mezzi illeciti o fraudolenti, ai servizi, ad altri account, ai sistemi o alle reti connesse.
4. L'Utente si impegna ad implementare, nel caso utilizzi una propria stazione di accesso alla posta elettronica, tutte quelle misure idonee e necessarie ad evitare, o comunque minimizzare, la divulgazione di virus informatici e simili.
5. L'Utente accetta di essere riconosciuto quale autore dei messaggi inviati dal suo account e di essere il ricevente dei messaggi spediti al suo account.

Art. 11 – Internet

1. È vietato navigare o registrarsi in siti non attinenti alle mansioni dell'Utente.
2. È vietato scaricare programmi o file musicali ancorché gratuiti.
3. È vietato partecipare a forum se non attinenti con la propria attività lavorativa e utilizzare chat line.
4. È vietato conservare file di contenuto discriminatorio e/o pedopornografico
5. È vietato fare acquisti su siti online utilizzando l'account istituzionale
6. Data la vasta gamma di attività, non è definito a priori un elenco di siti autorizzati;

Art. 12 – Computer

Nelle postazioni attive nell'istituto non è consentito:

1. installare programmi se non debitamente autorizzati;
2. modificare le configurazioni esistenti;
3. installare modem, router e switch o altri apparecchi se non debitamente autorizzati.
4. utilizzare supporti magnetici diversi da quelli appositamente autorizzati.

Ogni dispositivo magnetico di provenienza esterna all'istituto scolastico, dovrà essere verificato mediante programma antivirus prima del suo utilizzo.

Il Dirigente si riserva di effettuare controlli, anche attraverso l' Amministratore di Sistema o altri delegati, conformi alla legge, anche saltuari e occasionali, indicando le ragioni legittime – specifiche e non generiche – per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni). Per quanto concerne le prescrizioni sulla sicurezza dei dati e dei sistemi si rinvia alla documentazione interna dell'istituto.

Il Dirigente si riserva, altresì, di possibilità di controllo della posta quando strettamente necessario al fine di tutelare il patrimonio aziendale o verificare la commissione di un illecito.

Art. 13 - Controlli a distanza

In via generale, non sono consentiti i trattamenti effettuati mediante sistemi hardware e software che consentono il controllo dell'attività degli Utenti. Il divieto riguarda l'attività lavorativa e didattica in senso stretto e altre condotte personali poste in essere all'interno del luogo di lavoro.

A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili. Sono ovviamente vietati i sistemi preordinati al controllo diretto, che consentono di ricostruire l'attività di Utenti come nel caso di:

- Lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- Riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- Lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- Analisi occulta di computer portatili affidati in uso.

Altrettanto vietati sono i sistemi che consentono indirettamente il controllo, quando non sono preordinati a esigenze produttive od organizzative o, comunque, non siano necessari per la sicurezza sul lavoro.

In caso di necessità produttiva, organizzativa o di sicurezza, il trattamento dei dati che ne consegue può essere lecito, è però necessario rispettare le procedure di informazione e di consultazione di lavoratori e sindacati (di cui all'art. 4, comma 2, della L. 300/1970 aggiornata dal D.lgs 151/2015 e D.lgs 185/2016), in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.

Art. 14 - Graduazione dei controlli

Nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali degli Utenti, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura

personale o privata.

L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali.

Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale. Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

Art. 15 - Conservazione

I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovra-registrazione come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria. In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario – e predeterminato – a raggiungerla (v. art. 11, comma 1, lettera e) del Codice). Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione a:

- esigenze tecniche o di sicurezza del tutto particolari;
- indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria. In questi casi, il trattamento dei dati personali deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

Art. 16 - metadati

I "metadati" che "non vanno in alcun modo confusi con le informazioni contenute nei messaggi di posta elettronica nella loro "body-part" (corpo del messaggio) o anche in essi integrate" (tecnicamente si tratta di "informazioni registrate nei log generati dai sistemi server di gestione e smistamento della posta elettronica (MTA = Mail Transport Agent) e dalle postazioni client (MUA = Mail User Agent)", in altri termini, i metadati includono: indirizzi e-mail di mittente e destinatario, indirizzi IP dei server o client coinvolti, orari di invio, ritrasmissione o ricezione, dimensione del messaggio, presenza e dimensione di eventuali allegati e, a volte, l'oggetto del messaggio saranno conservati per un tempo massimo di 21 giorni come da normativa di settore (Provvedimento del 6 giugno 2024 - Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati [10026277])

Art. 17 - Sanzioni

In caso di abuso, o di inosservanza del presente regolamento, a seconda della gravità del fatto commesso e fatte salve le ulteriori conseguenze di natura disciplinare, penale, civile e amministrativa, saranno messi in atto i previsti interventi sanzionatori, regolativi e, laddove previsto, si procederà a segnalare il reato alle Autorità competenti.

Il Dirigente, in via provvisoria e di urgenza, in deroga all'art. seguente, può ordinare all'Amministratore di posta o al Fornitore l'immediata cessazione dell'attività all'origine dell'abuso, adottando le necessarie misure per impedire che l'abuso venga portato ad ulteriori conseguenze.

Nel caso b dell'articolo 9 c.1, e a seguito di segnalazione da parte dei gestori della rete, l'Istituto è autorizzato alla immediata sospensione dell'accesso senza preavviso. Nei casi c, e, f, g, i, l, dell'articolo 9 – c.1, l'Istituto è autorizzato alla immediata sospensione dell'accesso senza preavviso, dandone successivamente comunicazione al Dirigente.

Con l'entrata in vigore del presente Privacy Policy tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

-Copia di questo documento viene pubblicato sul sito istituzionale dell'Istituto, ed allegato alla comunicazione che ne ufficializza l'adozione nelle forme e con le modalità in uso presso l'Istituto.

*Il Dirigente scolastico
Prof. Luigi Nunziata*

Aggiornato al 14 Ottobre 2024