



## Ufficio d'Ambito di Como

Azienda Speciale ex art. 114 del D. Lgs. n. 267/2000 e smi  
con sede in Como – Via Borgo Vico n. 148  
Codice Fiscale: 95109690131  
Partita IVA: 03703830137  
Iscritto alla CCIAA di Como con R.E.A. n. 311161

# Regolamento di privacy policy per l'utilizzo della posta elettronica

Versione	Soggetto approvatore	delibera di n.	approvazione data
1	Delibera del CdA	17	26/02/2026

## Sommario

<b>INDICAZIONI GENERALI</b> .....	3
<b>ART. 1 – SCOPO</b> .....	4
<b>ART. 2 – AMBITO DI APPLICAZIONE</b> .....	4
<b>ART. 3 – CONDIZIONI GENERALI</b> .....	4
<b>ART. 4 – CONDIZIONI SPECIFICHE</b> .....	6
<b>4.1 – Avvertenze</b> .....	6
<b>4.2 – Uso consentito</b> .....	7
<b>ART. 5 – VIOLAZIONI</b> .....	7
<b>ART. 6 – PROCEDURA IN CASO DI RISOLUZIONE DEL CONTRATTO</b> .....	8
<b>ART. 7 – PROCEDURE PER DELEGHE IN CASO DI ASSENZE</b> .....	8
<b>ART. 8 – REGOLAMENTAZIONE BYOD</b> .....	9
<b>8.1 – Configurazione della posta su dispositivi personali</b> .....	9
<b>ART. 9 – NETIQUETTE</b> .....	10
<b>ART. 10 – NORME FINALI</b> .....	10
<b>ART. 11 – ENTRATA IN VIGORE</b> .....	11

## INDICAZIONI GENERALI

In materia di privacy ed e-mail dell'Azienda sono molteplici gli adempimenti necessari per una corretta gestione degli account nominativi da parte del Titolare del trattamento.

Gli account di posta composti da "nome e cognome", ancorché accompagnati dal dominio dell'Azienda, 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 n. 101/2018).

Detta condizione dipende, con tutta evidenza, dalla presenza nell'indirizzo di contatto non solo di dati formalmente personali, ma anche dall'effettivo uso che, indirettamente, potrebbe essere fatto dai dipendenti con riferimento ad uno strumento a conduzione prettamente individuale del singolo lavoratore, ma con risvolti comunque prevalentemente (ma non solo) professionali.

Per tale ragione, così come suggerito dal Garante (linee guida per posta elettronica e internet [doc. 1387522]), è buona norma rendere disponibili, prima di tutto, indirizzi di posta elettronica condivisi tra più lavoratori che richiamino con un buon grado di chiarezza il fatto che si tratta di un indirizzo di contatto "istituzionale" dell'Ente (es: info@ato.como.it, servizioxxxxx@ato.como.it, ecc), eventualmente affiancandoli a quelli individuali (nome.cognome@ato.como.it).

Questo perché nel caso in cui siano utilizzate e-mail condivise non sorgono tutte le problematiche relative alla tutela della riservatezza del lavoratore, ma solo alcune e ciò in quanto l'indirizzo di posta non contiene in sé alcun dato personale e non può presumersi un utilizzo personale dell'account.

La scelta dell'Azienda di assegnare ai lavoratori account di posta nominativi non è da escludere a priori o da eliminare, ma semmai è soltanto da regolamentare, e se del caso limitare.

In particolare, si ritiene opportuno prima di tutto indicare al lavoratore che **l'utilizzo dell'account nominativo deve avvenire per soli fini strettamente collegati all'attività dell'Azienda**, vietandone l'utilizzo privato.

È bene, infatti, tenere presente che un uso promiscuo, o non disciplinato, dell'account è senza dubbio fonte che genera dati personali del tutto estranei al contratto di lavoro instaurato dalle parti (i dati contenuti nelle e-mail – che possono essere strettamente personali, particolari o relativi a questioni riservate del lavoratore – inevitabilmente saranno salvati su server della società, su backup ecc.).

Tale circostanza rappresenta a tutti gli effetti un rischio privacy (ai sensi del GDPR, Reg. UE 2016/679) per il titolare e per l'interessato (il/la dipendente). Un rischio che se non adeguatamente mitigato può dar luogo a trattamenti di dati personali illegittimi, sanzionabili ai sensi del nuovo regolamento europeo e del Codice Privacy come riformato, o comunque a delle intromissioni – sia pure accidentali – nella sfera privata della risorsa umana.

La regolamentazione dell'uso della posta elettronica dell'Azienda rappresenta dunque non soltanto la misura idonea per evitare sanzioni derivanti dal trattamento di dati non pertinenti al rapporto di lavoro, ma allo stesso tempo è la miglior tutela per la riservatezza del lavoratore che terrà la propria corrispondenza personale fuori dal possibile e/o incidentale controllo datoriale che per legge può avvenire.

Infine si ricorda che l'Autorità Garante per la protezione dei dati personali prescrive ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lett. c), del Codice, di adottare la misura necessaria a garanzia degli interessati, riguardante l'onere di specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori, indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli.

Inoltre, ai Titolari del trattamento dei dati, viene ricordato l'adozione delle linee guida a garanzia degli interessati, per ciò che riguarda:

- a) l'adozione e la pubblicizzazione di un disciplinare interno;
- b) l'adozione di misure di tipo organizzativo.

La presente politica disciplina l'utilizzo del servizio di posta elettronica del dominio dell'Azienda, in conformità alle leggi vigenti e alle ulteriori disposizioni emanate dall'Azienda.

Nella definizione delle regole d'uso del servizio di posta elettronica e delle modalità di controllo, si ritiene di grande importanza salvaguardare la libertà di espressione e di pensiero e la garanzia della privacy dell'individuo. Questa politica rispetta quindi i principi basilari esposti, nel contesto delle obbligazioni legali e delle politiche di sicurezza dell'Azienda.

L'Azienda, anche sulla base delle direttive del governo tese a promuovere la crescita delle comunicazioni in formato digitale e l'abbattimento di quelle cartacee, considera la posta elettronica uno strumento fondamentale, che viene messo a disposizione di tutti coloro che ne abbiano diritto.

## **ART. 1 – SCOPO**

Scopo della presente politica è assicurare che:

- gli utenti del servizio di posta elettronica siano informati delle disposizioni di legge vigenti e della giurisprudenza relativa alla disciplina dell'uso della posta elettronica;
- il servizio di posta elettronica sia utilizzato dagli utenti in conformità a tali disposizioni;
- gli utenti del servizio di posta elettronica siano informati in merito ai concetti di protezione dei dati personali e di sicurezza applicabili all'uso della posta elettronica;
- il servizio di posta e altri servizi siano fruibili con la massima continuità ed affidabilità.

## **ART. 2 – AMBITO DI APPLICAZIONE**

La presente politica si applica ai servizi di posta elettronica dell'Azienda e a tutti gli utenti dotati di una casella di posta elettronica, definita nel dominio "ato.como.it", appartenenti alle seguenti categorie di personale:

- direttore
- dipendenti dell'Azienda
- consiglieri
- presidente
- ogni altra categoria di personale, cui venga fornito in modo temporaneo un account di posta elettronica per lo svolgimento delle proprie attività.

La presente politica si applica indifferentemente ai contenuti dei messaggi di posta e alle informazioni transazionali (header dei messaggi, indirizzi di posta, dati dei destinatari e dei mittenti) relative a tali messaggi.

## **ART. 3 – CONDIZIONI GENERALI**

- a) **Finalità del servizio di posta elettronica:** l'Azienda incoraggia l'uso delle tecnologie al fine di migliorare le comunicazioni, scambiare idee e per rendere più efficaci ed efficienti i processi di lavoro a supporto della missione istituzionale dell'Azienda.
- b) **Proprietà:** il servizio di posta elettronica dell'Azienda associata al dominio, erogato per il tramite dei Fornitori dei servizi in outsourcing, è di proprietà dell'Azienda stessa.

c) **Restrizioni all'uso del servizio:** gli utenti del servizio di posta elettronica sono tenuti ad usarlo in modo responsabile, cioè, rispettando le leggi, la presente e altre politiche loro indicate e secondo normali standard di cortesia, correttezza, buona fede e diligenza professionale. L'accesso ai servizi di posta elettronica dell'Azienda può essere totalmente o parzialmente limitato dall'Azienda stessa, senza necessità di assenso da parte dell'utente e anche senza preavviso:

- quando richiesto dalla legge e in conformità ad essa;
- in caso di comprovati motivi che facciano ritenere la violazione della presente politica o delle disposizioni di legge vigenti;
- al venir meno delle condizioni in base alle quali si ha facoltà di utilizzare il servizio (ad es. cessazione per qualsiasi motivo del rapporto di lavoro con l'Azienda);
- in casi eccezionali, quando richiesto per esigenze operative critiche e improcrastinabili, debitamente motivate al diretto interessato.

L'accesso ai servizi di posta elettronica deve essere disattivato dall'Azienda in caso di cessazione del rapporto di lavoro.

d) **Controlli e accesso dei messaggi di posta:** nel pieno rispetto delle previsioni dello Statuto dei lavoratori, delle pronunce del Garante per la Protezione dei Dati Personali (Garante Privacy), e della dignità e libertà dei lavoratori, l'Azienda può riservarsi di controllare (direttamente o attraverso la propria struttura) il corretto utilizzo degli strumenti di lavoro (v. anche artt. 2086, 2087 e 2104 cod. civ.) quando ciò risulti connesso a specifiche esigenze organizzative, produttive e di sicurezza del lavoro, o per dare attuazione all'esercizio di un diritto in sede giudiziaria.

L'Azienda, invero, si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, anche per verifiche sulla funzionalità e sicurezza del sistema: in caso di abusi singoli o reiterati, potranno essere inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni.

Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o organizzative (ad es., per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2), di sistemi che consentono indirettamente un controllo a distanza, anche in presenza di attività di controllo discontinue. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati.

Si specifica che nell'effettuare controlli sull'uso degli strumenti elettronici l'Azienda deve evitare un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, 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. Verrà, per quanto possibile, preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Il controllo anonimo potrà 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 potrà 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.

l. **Asenso e Conformità:** l'Azienda è tenuta ad ottenere l'assenso del titolare della casella di posta elettronica prima di ogni ispezione dei messaggi o di accesso alle registrazioni o ai messaggi di

posta elettronica, fatta eccezione per quanto disposto al punto e). D'altro canto, ci si attende che il personale soddisfi le richieste dell'Azienda riguardanti la fornitura di copie delle registrazioni di posta elettronica in suo possesso che riguardino le attività lavorative richieste per soddisfare obblighi di legge, indipendentemente dal fatto che tali registrazioni risiedano o meno su computer di proprietà dell'Azienda. La condotta operativa qui definita da parte dell'Azienda deve essere ispirata ad una stretta e rigorosa applicazione dei principi di pertinenza e di non eccedenza, contemperando le esigenze di ordinato esercizio dell'attività aziendale con il diritto alla riservatezza dell'interessato.

- II. **Limitazioni all'accesso senza assenso:** l'Azienda non ispeziona e non accede ai messaggi di posta elettronica dell'utente senza la sua autorizzazione. L'Azienda permetterà l'ispezione, il monitoraggio o l'accesso alla posta elettronica degli utenti, anche senza l'assenso del titolare, solamente nei seguenti casi:
- su richiesta scritta dell'autorità giudiziaria nei casi previsti dalla normativa vigente;
  - previo preavviso all'utente, per gravi e comprovati motivi che facciano credere che siano state violate le disposizioni di legge vigenti o le politiche in materia di sicurezza e protezione dei dati personali, quando si ravveda dal bilanciamento di interessi tra le parti la prevalenza del legittimo interesse del titolare del trattamento
  - per atti dovuti, quando si ravveda dal bilanciamento di interessi tra le parti la prevalenza del legittimo interesse del titolare del trattamento
  - in situazioni critiche e di emergenza, debitamente motivate al diretto interessato, quando si ravveda dal bilanciamento di interessi tra le parti la prevalenza del legittimo interesse del titolare del trattamento.
- III. **Gestione dei Log:** il fornitore del servizio di posta elettronica registra e conserva i dati delle caselle di posta elettronica messe a disposizione dei propri utenti, tramite scrittura in appositi file di log, delle seguenti informazioni minime per ogni messaggio:
- mittente;
  - destinatario/i;
  - giorno ed ora dell'invio esito dell'invio;
  - operazioni effettuate sui messaggi;
  - operazioni effettuate sull'account di posta;
  - accessi alla casella (login, log out).

Resta a carico dell'Azienda il compito di garantire che i sistemi informatici vengano programmati e configurati con dei criteri tali da rispettare i termini di conservazione presenti in materia di accessi ad internet e traffico telematico non ritenuti necessari.

## ART. 4 – CONDIZIONI SPECIFICHE

### 4.1 – Avvertenze

Gli utenti del servizio di posta elettronica sono avvisati del fatto che:

- a) La natura stessa della posta elettronica la **rende meno sicura di quanto** si possa immaginare. Ad esempio, i messaggi di posta elettronica spediti ad una persona possono essere facilmente inoltrati ad altri destinatari. Ne l'Azienda né il fornitore del servizio possono proteggere gli utenti da fatti come quelli descritti che esulano dalle proprie possibilità e compiti. Gli utenti pertanto devono esercitare la **massima cautela** nell'uso della posta elettronica per **comunicare informazioni riservate**.

- b) I messaggi di posta elettronica, creati e conservati sia su apparati elettronici forniti dall'Ente che su altri sistemi (BYOD), possono costituire registrazioni di attività svolte dall'utente nell'espletamento delle sue attività lavorative. È possibile quindi che venga richiesto di accedere ai contenuti dei messaggi per un eventuale utilizzo nell'ambito di contenziosi che coinvolgano l'Azienda. L'Azienda non darà corso automaticamente a tutte le richieste di accesso, ma le valuterà in relazione a precisi obblighi normativi riferibili alla protezione dei dati personali ed altre disposizioni applicabili in materia, ma sempre con un'azione ispirata ad una stretta e rigorosa applicazione dei principi di pertinenza e di non eccedenza.
- c) Non c'è garanzia, a meno di utilizzare sistemi di posta certificata, che i messaggi ricevuti provengano effettivamente dal mittente previsto, perché è piuttosto semplice per i mittenti mascherare la propria identità. Inoltre, i messaggi di posta che arrivano come "inoltro" di precedenti messaggi, potrebbero essere stati modificati rispetto all'originale. Pertanto, in caso di dubbi, chi riceve un messaggio di posta elettronica dovrebbe verificare con il mittente l'autenticità delle informazioni ricevute.
- d) Per garantire la massima sicurezza e tracciabilità nelle comunicazioni ufficiali dell'Azienda, è fortemente raccomandato l'utilizzo della **Posta Elettronica Certificata (PEC)**. La PEC offre vantaggi significativi in termini di validità legale, integrità dei contenuti e conferma di avvenuta consegna, rendendola lo strumento ideale per scambi formali tra l'Azienda, i suoi dipendenti e soggetti esterni.

#### 4.2 – Uso consentito

L'uso del servizio di posta elettronica è soggetto alle seguenti condizioni:

- a) **Divieti.** È fatto divieto a tutti gli utenti di utilizzare il servizio di posta elettronica per inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione dell'Azienda. È inoltre vietato l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali e la fornitura (gratuita o a pagamento) a persone fisiche o giuridiche. È proibito fornire le proprie credenziali di accesso a sistemi o procedure, così come rispondere a messaggi e-mail che facciano richiesta di questo tipo di informazioni. Chiunque riceva comunicazioni della natura sopra indicata dovrà prontamente provvedere a verificare e cancellare il messaggio stesso; chiunque dovesse inviare comunicazioni del tipo sopra presentato potrà essere sottoposto a procedimento disciplinare, oltre a risponderne – laddove ne fossero rilevati i presupposti – davanti alle competenti Autorità. Sul punto, si rimanda anche al successivo Art. 5.
- b) **Uso Personale.** È vietato l'utilizzo del proprio account per fini privati e personali. L'utente è edotto del fatto che l'Azienda considererà, ai fini di eventuali ispezioni, tutti i messaggi di posta elettronica da lui gestiti come strettamente afferenti all'uso del servizio per scopi di lavoro.

#### ART. 5 – VIOLAZIONI

Il personale che contravviene alle norme indicate nel presente documento, stanti le responsabilità individuali di tipo civile e penale verso terze parti offese, potrà essere oggetto di sanzioni di tipo amministrativo la cui entità e modalità di erogazione saranno definite secondo le procedure previste dal contratto di lavoro attualmente vigente.

## ART. 6 – PROCEDURA IN CASO DI RISOLUZIONE DEL CONTRATTO

Riveste vitale importanza la questione relativa agli effetti, sulla gestione degli account, delle risoluzioni contrattuali fra lavoratore e datore di lavoro e in particolare in quei casi in cui repentinamente (ossia in tronco) cessa il rapporto di lavoro (dimissioni o licenziamento per giusta causa).

In linea con quanto suggerito dal Garante per la protezione dei dati, l'Azienda provvederà per l'account nominativo ad informare coloro i quali dovessero entrarvi in contatto, con un messaggio impostato con il risponditore automatico, che le comunicazioni lavorative, indirizzate all'account in disattivazione, potranno essere da quel momento in avanti inviate ad un diverso indirizzo, il cui contatto, già in quella sede, verrà reso noto con il medesimo messaggio di risposta automatica.

La casella di posta elettronica nominativa dovrà essere tempestivamente dismessa dall'Amministratore di sistema (ADS), appositamente nominato. .

- a) **Disattivazione:** nei limiti dei principi di proporzionalità e limitazione del trattamento l'Azienda potrà mantenere attivo il precedente account per un periodo limitato, che comunque non potrà superare 1 mese.
- b) **Accesso:** l'accesso all'account sarà completamente disabilitato per tutti gli utenti, senza eccezioni. Qualsiasi tentativo di utilizzo non autorizzato o accesso delegato da parte di terzi sarà considerato una violazione delle politiche aziendali e potrà comportare sanzioni disciplinari.
- c) **Delega:** è espressamente vietata la delega a terzi per l'utilizzo della posta elettronica personale o dell'account di lavoro durante il periodo di attività residua.
- d) **Eliminazione:** al termine del mese di attività residua, la casella di posta e tutti i dati in essa salvati saranno eliminati.

## ART. 7 – PROCEDURE PER DELEGHE IN CASO DI ASSENZE

In caso di assenza programmata del lavoratore per un periodo prolungato (ad es. per ferie), la stessa dovrà essere tempestivamente comunicata, così da poter attivare apposite funzionalità di sistema che consentano di inviare automaticamente messaggi di risposta che contengano le "coordinate" di altro soggetto (collega fiduciario o indirizzo e-mail generico dell'Azienda o del Servizio di riferimento) o altre utili modalità di contatto.

In caso di eventuali assenze non programmate (ad es. per malattia), qualora il lavoratore non possa attivare la procedura sopra descritta (anche avvalendosi di servizi webmail), il titolare del trattamento, potrà disporre lecitamente, mediante personale appositamente incaricato (ad es. l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento.

Laddove, in caso di una assenza improvvisa o prolungata coincidente con delle improrogabili necessità legate all'attività e al buon funzionamento dell'Azienda, occorra conoscere il contenuto dei messaggi di posta elettronica, l'interessato sarà messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare all'Azienda quelli ritenuti rilevanti per lo svolgimento dell'attività della medesima; di tale attività l'Azienda avrà cura di redigere un apposito verbale, da somministrare in copia al lavoratore interessato alla prima occasione utile per una sua sottoscrizione. In entrambi i casi sopra descritti, i messaggi di posta elettronica inoltrati dal risponditore automatico è bene che contengano un avvertimento ai destinatari degli stessi a mezzo dei quali venga dichiarata l'eventuale natura non personale dei messaggi stessi, precisando che le risposte potranno essere

conosciute nell'organizzazione di appartenenza del mittente con eventuale rinvio alla predetta policy datoriale.

## **ART. 8 – REGOLAMENTAZIONE BYOD**

In considerazione che il BYOD genera un rischio elevato per i dati e pertanto abbassa la sicurezza dei dati dell'Azienda; in particolare si avrà:

- local exposure: la perdita di controllo dei dati aziendali, che vengono trasmessi, archiviati ed elaborati sui dispositivi personali dei dipendenti;
- Perdita di dati: il BYOD può portare alla potenziale perdita o divulgazione dei dati aziendali da un dispositivo non protetto oppure causata dal furto del dispositivo;
- esposizione pubblica dei dati: usare dispositivi personali per attività d'ufficio aumenta il rischio di attacchi e intercettazione dei dati, soprattutto quando il dipendente si connette via hotspot, wi-fi pubblico o tramite Bluetooth;
- app dannose: un esempio sono le notifiche push che possono compromettere le applicazioni attendibili sul dispositivo;
- personalizzazione delle impostazioni di sicurezza: gli utenti di dispositivi ad uso personale solitamente rimuovono le restrizioni imposte dai fornitori, ma così facendo rendono il dispositivo più vulnerabile alle applicazioni non sicure, che accedono ai dati aziendali.

Per quanto concerne l'utilizzo di dispositivi personali (BYOD Bring your own device) per l'accesso agli account di posta elettronica dovrà essere preventivamente autorizzato e annotato in apposito registro. L'Azienda si riserva di revocare le singole autorizzazioni concesse laddove vengano meno i presupposti in fatto e/o in diritto del perdurare delle stesse.

Il dispositivo dovrà essere custodito e utilizzato con la massima cura e attenzione, secondo il principio della diligenza del buon padre di famiglia, poiché contiene dati sensibili e informazioni dell'Azienda.

**In caso di cessazione del rapporto di lavoro**, tutti i dati relativi all'Azienda contenuti nei dispositivi personali dovranno essere immediatamente eliminati e distrutti dall'utente, in conformità con le normative vigenti sulla protezione dei dati.

**In caso di furto del dispositivo BYOD**, l'utente è tenuto a notificare tempestivamente l'accaduto al Responsabile del Servizio Amministrativo finanziario dell'Azienda e al Direttore. Questo consentirà di avviare immediatamente la procedura di cancellazione remota della posta elettronica lavorativa, al fine di prevenire accessi non autorizzati e tutelare la riservatezza delle informazioni aziendali.

### **8.1 – Configurazione della posta su dispositivi personali**

La configurazione della posta elettronica su dispositivi personali può avvenire in due modalità:

- a. **Utilizzo del client di posta nativo**: In questo caso, l'amministratore di sistema ha la facoltà di eseguire un reset completo del dispositivo, ripristinandolo alle impostazioni di fabbrica, qualora necessario per ragioni di sicurezza o conformità.
- b. **Utilizzo del client ufficiale Microsoft Outlook**: In questa modalità, l'amministratore potrà limitarsi a cancellare esclusivamente i dati relativi alla posta elettronica dal dispositivo, senza influire sugli altri dati personali memorizzati.

## ART. 9 – NETIQUETTE

Le regole dettate dalla Netiquette sono specificate in un documento ufficiale (RFC-1855) che è stato scritto nel lontano 1995.

Di seguito vengono riportate le parti fondamentali rielaborate e adattate ai giorni nostri, di seguito vengono elencate post le regole di **netiquette** legate alla scrittura delle email:

- Si scrive sempre in **minuscolo**: il MAIUSCOLO viene interpretato come un messaggio “urlato”;
- È consigliabile usare solo caratteri alfanumerici di uso comune e non utilizzare caratteri speciali che non sempre sono interpretati correttamente dal destinatario;
- È buona norma **limitare la lunghezza** del messaggio, soprattutto se si risponde ad una mail ricevuta. Riportare il messaggio originale solo se strettamente necessario ed eventualmente ripulitelo da eventuali immagini, firme e contorni grafici accessori;
- Quando scriviamo delle battute nel messaggio di testo è in assoluto consigliato l’utilizzo degli **smiley** 😊 perché aiuta a delinearne il contorno ironico e non viene frainteso il messaggio. Ovviamente diverso è il comportamento per le mail a carattere formale dove sono invece assolutamente sconsigliati l’uso degli emoticon (vedi smiley...) perché rischiano di creare un alone poco professionale a ciò che vogliamo comunicare;
- Scrivere sempre l’**oggetto** della mail, perché è cortese dare la possibilità al destinatario di sapere a colpo d’occhio la motivazione per cui gli avete scritto;
- Rispettate la **privacy** del mittente/destinatario, cancellando dal testo della mail eventuali indirizzi di posta elettronica o riferimenti personali altrui nel caso in cui la mail dovesse essere inoltrata a un destinatario diverso da quelli originariamente inseriti;
- Utilizzate il **campo CC** (copia conoscenza) mettendo al massimo due destinatari che si conoscono tra loro o che dobbiamo presentare, altrimenti utilizzare il campo CCn. Se è necessario inviare informazioni a molti destinatari è consigliato creare una lista di distribuzione (gruppo di destinatari);
- Utilizzate il **campo CCn** (copia conoscenza nascosta) se è necessario inviare la stessa mail a destinatari diversi che non si conoscono tra loro;
- È consigliato inviare mail di **testo** semplici senza contorni grafici e disegni. La mail sarà sicuramente più leggibile e chiara;
- Ad oggi la maggior parte dei provider di posta permettono di inviare **allegati** per mail fino a 25 MB. È comunque cortesia avvisare prima il destinatario quando si ha intenzione di inviare un messaggio con un “peso” importante;
- La posta elettronica è facilmente intercettabile quindi non scrivere mai **dati sensibili** come carte di credito, password, etc. In caso di necessità utilizzare dei programmi di crittografia;
- Non utilizzate la posta elettronica come mezzo di offesa, per diffondere spam o per altri **usi illeciti** o non etici. È fatto divieto partecipare alla diffusione di catene di S. Antonio;
- Fate attenzione alla **grammatica e all’ortografia**;
- Quando scrivete di getto, salvate la mail come bozza, e poi rileggerla con calma;
- Rileggete almeno tre volte avete ciò che scritto prima di inviarlo;
- È cortesia rispondere a una mail entro 24-48 ore dalla sua ricezione.

## ART. 10 – NORME FINALI

Per tutto quanto non espressamente previsto dal presente Regolamento, si rinvia alle disposizioni di legge vigenti in materia nel tempo.

**ART. 11 – ENTRATA IN VIGORE**

Il presente Regolamento entrerà in vigore contestualmente all'intervenuta esecutività della relativa deliberazione di approvazione da parte del CdA dell'Azienda.

Esso potrà essere modificato in qualsiasi momento, in funzione di intervenute diverse esigenze aziendali o normative.