COMUNE DI PIATEDA

REGOLAMENTO

DI UTILIZZO DEL

SISTEMA INFORMATICO

COMUNALE (S.I.C.)

Approvato con Deliberazione di Giunta Comunale n. 93 del 01.12.2021

I N D I C E

Articolo 1 – Riferimenti

I riferimenti normativi del presente regolamento sono i seguenti:

- Regolamento (UE) n. 2016/679, General Data Protection Regulation (GDPR)
- Provvedimento a carattere generale del Garante del 27 novembre 2008 dal titolo "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", pubblicato sulla G.U. n. 300 del 24 dicembre 2008.

Il regolamento tiene inoltre conto di quanto disposto dal "Modulo di implementazione" allegato alla Circolare 18 aprile 2017, n. 2/2017, recante “Misure minime di sicurezza ICT per le pubbliche amministrazioni” (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015).

Articolo 2 – Definizioni

Ai fini dell’applicazione del presente regolamento deve intendersi per:

Sistema Informatico Comunale (di seguito S.I.C.): l'insieme degli strumenti tecnologici utilizzati dal Comune per il trattamento e la conservazione delle informazioni, composto dalle singole postazioni di lavoro, da elementi hardware (server di rete, stampanti, periferiche, ecc.), software (programmi informatici di base e applicativi, database, ecc.) e reti telematiche.

Titolare del Trattamento dei dati personali (Titolare): persona fisica cui competono le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Per il Comune di Piateda, il legale rappresentante dell’ente, individuato nel Sindaco pro-tempore.

Amministratore di Sistema (AdS): figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione dati, all’amministrazione di basi di dati, di reti, di apparati di sicurezza e di sistemi software complessi. Tale figura è ricoperta da personale interno, con il supporto della Comunità Valtellina di Sondrio, con la quale il Comune ha sottoscritto apposita convenzione per la gestione in forma associata, tra l’altro, anche del sistema di informatizzazione.

Utente: persona che a qualsiasi titolo accede, anche in forma parziale o per limitati periodi di tempo, al S.I.C.

Articolo 3 - Informazioni e norme generali

Gli utenti del S.I.C. sono formalmente autorizzati dall’Amministrazione e tecnicamente abilitati dall’AdS. Non è consentito alcun accesso anonimo o non autorizzato.
Ogni utente è tenuto ad osservare il presente regolamento al fine di preservare la funzionalità e la sicurezza del sistema stesso e delle informazioni gestite e conservate; a tal fine ogni utente riceve copia integrale del presente documento e firma l’allegato modulo per presa visione e accettazione.
Gli strumenti informatici possono essere utilizzati unicamente per gli scopi definiti dall'Amministrazione e comunque per lo svolgimento delle attività d’ufficio proprie di ciascun dipendente.

Articolo 4 - Norme tecniche

Postazioni di lavoro
Ogni postazione di lavoro viene installata con una configurazione adatta alle specifiche esigenze delle varie realtà lavorative, concordata dai Responsabili di Servizio con l'AdS.
La postazione si compone di:

- dotazione hardware e software;
- impostazioni utente (salvaschermo, memorizzazione password, ecc.);
- autorizzazione per l'accesso a cartelle condivise e software applicativi.

Qualsiasi variazione alla configurazione della postazione di lavoro (ad esempio l'installazione di nuovi software o la rimozione o aggiornamento di quelli presenti, la modifica delle impostazioni utente, ecc.) deve essere preventivamente autorizzata dal Responsabile di Area e concordata con l'AdS.
Non è consentito il collegamento al S.I.C. di apparecchiature non di proprietà dell'Amministrazione, salvo specifica autorizzazione dell'AdS.

Credenziali utente
Ciascun utente del S.I.C. si connette alla rete, alle piattaforme software e alla posta elettronica, tramite autenticazione univoca personale. L'utente è tenuto a custodire e garantire la segretezza della parola chiave e a sostituirla almeno ogni sei mesi.
Le password sono modificabili da tutti gli utenti in qualsiasi momento tramite apposita procedura, specifica di ogni contesto applicativo.
I requisiti minimi di complessità delle password sono:

- redazione con caratteri maiuscoli e minuscoli
- composizione con inclusione di lettere, numeri e simboli o segni di punteggiatura
- numero caratteri non inferiori ad 8
- password non agevolmente riconducibile all'identità del soggetto che la gestisce.

Il Titolare del trattamento dati personali può richiedere all'AdS la disponibilità di dati o strumenti elettronici assegnati ad un utente in caso di sua prolungata assenza o di impedimento. Ciò avviene attraverso la sostituzione della password effettuata dall'AdS che la comunica al Titolare. L'AdS comunica tempestivamente e per iscritto all'utente l'avvenuto cambio delle credenziali di accesso e le motivazioni.

Gestione dei dati
La rete interna, istituita appositamente per permettere collegamenti funzionali tra gli utenti, non può esser utilizzata per scopi diversi da quelli ai quali è destinata.
Le cartelle di rete sono sottoposte a procedure di backup e controllo degli accessi e sono l'unico supporto sicuro sul quale memorizzare i documenti elettronici. L'utilizzo da parte degli utenti di qualsiasi altro supporto di memorizzazione (ad esempio le cartelle locali del personal computer) non garantisce la sicurezza del dato in caso di guasti hardware, sovrascritture o cancellazioni accidentali, attacchi informatici di virus o altri software malevoli.
Qualsiasi file estraneo all'attività lavorativa, se non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato nelle cartelle di rete.
Tutti i file di provenienza incerta o comunque esterna (Internet, posta elettronica, supporti rimuovibili), ancorché attinenti l'attività lavorativa, devono essere sottoposti al controllo antivirus. E' vietata la cifratura di documenti effettuata autonomamente dall'utente se non concordata e autorizzata dall'AdS.

Utilizzo rete Internet
L'accesso a Internet è possibile da qualsiasi postazione connessa alla rete e costituisce parte integrante della dotazione informatica di ogni utente.

Non è consentito l'accesso a siti, social network o qualsiasi altro tipo di risorsa on-line, per scopi non inerenti la propria attività lavorativa, salvo autorizzazione concordata con l'Amministrazione Comunale.
L'Amministrazione Comunale può inoltre avvalersi di sistemi in grado di documentare il traffico internet generato dalle stazioni di lavoro. Tali informazioni sono raccolte unicamente allo scopo di verificare ex-post utilizzi illeciti del collegamento ad Internet; il loro accesso è consentito unicamente al Titolare del trattamento dati personali e si effettuerà unicamente nei modi previsti dalla legge ed in particolare secondo principi di gradualità dei controlli, pertinenza e non eccedenza.

Utilizzo posta elettronica
Il comune di Piateda ha fornito ai propri lavoratori solo ed esclusivamente account di posta elettronica condivisi tra più lavoratori e appartenenti al dominio istituzionale (comune.piateda.so.it). Gli stessi sono di esclusiva proprietà dell'Amministrazione Comunale e il loro utilizzo è autorizzato solo per esigenze di servizio.
Lo strumento della posta elettronica è fondamentale 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'Ente pur non sostituendo altri sistemi più idonei per l'interscambio di documenti. L'invio di allegati è consentito solo per file con dimensioni contenute (fino a un massimo di 25 Mb).

Le modalità di utilizzo del servizio e-mail dell'Ente sono definite nel documento "Privacy policy di utilizzo del servizio e-mail dell'Ente" allegato al presente regolamento (allegato B).

Portale Internet comunale
Gli utenti autorizzati possono pubblicare pagine informative e modulistica sul portale Internet comunale, utilizzando gli strumenti di redazione messi a disposizione dal S.I.C.
Ogni utente è responsabile dei contenuti da esso pubblicati ed è tenuto a verificarli prima dell'effettiva pubblicazione, al fine di garantire la tutela dell'ente.

Protezione antivirus
Ogni utente è tenuto a tenere comportamenti tali da ridurre il rischio di attacco al S.I.C. da parte di virus o di ogni altro software malevolo che operi con lo scopo di superare le difese di sicurezza del sistema stesso.
A tal fine, ogni utente è tenuto a:

- evitare tassativamente l'apertura di file allegati ad e-mail provenienti da utenti sconosciuti o contenenti messaggi sospetti
- segnalare tempestivamente all'AdS eventuali avvisi di rischio ricevuti dal software antivirus installato o altre anomalie di funzionamento del sistema
- evitare la navigazione Internet su siti non istituzionali o la cui affidabilità non è accertabile
- ridurre allo stretto necessario l'utilizzo di dispositivi rimuovibili personali (USB drive, CD/DVD o simili)
- controllare, mediante il software antivirus, il contenuto di supporti rimuovibili autorizzati prima di ogni utilizzo

Accesso ad archivi contenenti dati personali
Il Comune di Piateda, per perseguire le proprie finalità istituzionali, gestisce archivi contenenti dati personali tutelati dalla normativa in materia di Privacy.
L'accesso agli archivi contenenti dati personali (comuni e/o sensibili) è consentito esclusivamente agli utenti autorizzati, identificati tramiti le proprie credenziali di accesso al sistema.
Ogni utente è tenuto a non allontanarsi dal proprio posto di lavoro senza aver prima chiuso la propria sessione di lavoro o bloccato in altro modo l'accesso non autorizzato al proprio sistema.

Utilizzo dei materiali di consumo
L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, CD, DVD) è riservato esclusivamente a funzioni inerenti l'attività lavorativa.
Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

Articolo 5 – Responsabilità

L'utente è informato del fatto che la conoscenza delle credenziali di autenticazione da parte di terzi consentirebbe a questi ultimi l'utilizzo del sistema informativo e dei servizi erogati attraverso di esso, pertanto è tenuto a non rivelare ad alcuno le proprie credenziali di autenticazione per l'accesso al sistema informativo.
L'utente è il solo ed unico responsabile della conservazione e della riservatezza delle proprie credenziali di autenticazione e, conseguentemente, rimane il solo ed unico responsabile per tutti gli usi ad essa connessi o correlati, (ivi compresi danni e conseguenze pregiudizievoli arrecati all'ente e/o a terzi) siano dal medesimo utente autorizzati ovvero non autorizzati.
L'utente si impegna a comunicare immediatamente all'AdS l'eventuale furto, smarrimento o perdita della password. In particolare, in caso di furto, l'utente si impegna a modificare tempestivamente tale password utilizzando le procedure automatiche a sua disposizione.

Articolo 6 – Sanzioni

Qualsiasi utilizzo del S.I.C. non conforme alle disposizioni del presente regolamento e/o alle leggi vigenti è ad esclusiva responsabilità dell'utente.
Nei casi in cui si accertino violazione del regolamento, è demandata ai rispettivi Responsabili l'applicazione dei necessari provvedimenti disciplinari, fermo restando l'obbligo di segnalare al Titolare, al Segretario Comunale ed alla competente autorità giudiziaria eventuali violazioni costituenti reato.

COMUNE DI PIATEDA
Provincia di Sondrio

Allegato A - Modulo di presa visione e accettazione

PRESA VISIONE ED ACCETTAZIONE DEL REGOLAMENTO DI UTILIZZO DEL SISTEMA INFORMATICO COMUNALE

Il/La sottoscritto/a _____,

nato/a _____ il _____,

residente a _____ in via _____,

telefono _____ codice fiscale _____,

d i c h i a r a

di aver preso visione ed accettare tutte le norme contenute nel regolamento di utilizzo del Sistema Informatico del Comune di Piateda.

Data _____ Firma _____

Allegato B

PRIVACY POLICY DI UTILIZZO DEL SERVIZIO E-MAIL DELL'ENTE

PREMESSO CHE

Il Comune di Piateda ha fornito ai propri lavoratori solo ed esclusivamente indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@comune.piateda.so.it, tecnico@comune.piateda.so.it, etc.), così come suggerito dal Garante della Privacy (linee guida per posta elettronica e internet [doc. 1387522]).
La scelta dell'Ente è quella di non assegnare, nemmeno in futuro, ai lavoratori account di posta nominativi al fine di non far sorgere tutte le problematiche relative alla tutela della riservatezza del lavoratore stesso, in quanto l'indirizzo di posta condiviso non contiene in sé alcun dato personale e non può, altresì, presumersi un utilizzo personale dell'account.
La presente politica disciplina l'utilizzo del servizio di posta elettronica del dominio dell'Ente, in conformità alle leggi vigenti anche in materia di protezione dei dati personali e alle ulteriori disposizioni emanate dall'Amministrazione, tenuto conto che la stessa Amministrazione, 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:

1. 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;
2. il servizio di posta elettronica sia utilizzato dagli utenti in conformità a tali disposizioni;
3. gli utenti del servizio di posta elettronica siano informati in merito ai concetti di privacy e di sicurezza applicabili all'uso della posta elettronica;
4. 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'Ente e a tutti gli utenti dotati di una casella di posta elettronica, definita nel dominio "**comune.piateda.so.it**".

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

Finalità del servizio di posta elettronica: L'Ente 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'Ente.

Proprietà: il servizio di posta elettronica dell'Ente associata al dominio, erogato per il tramite dei Fornitori dei servizi in outsourcing, è di proprietà dell'Ente stesso.

Restrizioni all'uso del servizio. Gli utenti del servizio di posta elettronica sono tenuti ad usarlo in modo responsabile, 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'Ente può essere totalmente o parzialmente limitato dall'Ente stesso, 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'Ente)
- in casi eccezionali, quando richiesto per esigenze operative critiche e improcrastinabili.

Assenso e Conformità. L'Ente è tenuto ad ottenere l'assenso degli utilizzatori 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 successivo punto. D'altro canto, ci si attende che il personale soddisfi le richieste dell'Ente 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'Ente.

Limitazioni all'accesso senza assenso. L'Ente non ispeziona e non accede ai messaggi di posta elettronica dell'utente senza la sua autorizzazione. L'Ente permetterà l'ispezione, il monitoraggio o l'accesso alla posta elettronica degli utenti, anche senza l'assenso dell'utente, 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 privacy
- per atti dovuti
- in situazioni critiche e di emergenza.

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 effettuati sui messaggi
- operazioni effettuati sull'account di posta
- accessi alla casella (login, log out)

I file di registro sono conservati per un periodo non inferiore ai 180 giorni.

Art. 4 – CONDIZIONI SPECIFICHE

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

- 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'Ente 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 o dati sensibili.**
- I messaggi di posta elettronica, creati e conservati sia su apparati elettronici forniti dall'Ente che su altri sistemi di condivisione dei dati tra dispositivi (BYOD – Bring Your Own Device), 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'Amministrazione. L'Ente non darà corso automaticamente a tutte le richieste di accesso, ma le valuterà in relazione a precisi obblighi di legge quali la privacy ed altre normative applicabili.
- 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.

Divieti. È fatto divieto a tutti gli utenti di:

- utilizzare il servizio di posta elettronica per inviare messaggi dannosi, di tipo offensivo o sconveniente;
- utilizzare il servizio di posta elettronica per fini privati e personali, nonché per fini commerciali o di profitto personale e per attività illegali;
- 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.

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 – REGOLAMENTAZIONE BYOD - Bring Your Own Device - "porta il tuo dispositivo"

Il BYOD prevede l'incorporazione delle tecnologie di diversi dispositivi sia personali che di carattere aziendale di ambito sia pubblico che privato (ad esempio con una politica di BYOD un'azienda può consentire ai propri dipendenti di svolgere il lavoro sia in ufficio che al di fuori di esso e in orari flessibili).

In considerazione che il BYOD presenta alcuni inconvenienti soprattutto a livelli di sicurezza quali:

- la possibile perdita di controllo dei dati aziendali, che vengono trasmessi, archiviati ed elaborati su dispositivi personali dei dipendenti anche a causa della rimozione delle impostazioni di sicurezza;
- la possibile perdita o la divulgazione dei dati aziendali da un dispositivo non protetto o a causata dal furto del dispositivo stesso;
- la possibile esposizione pubblica dei dati a causa dell'utilizzo di dispositivi personali per attività d'ufficio che sono maggiormente esposti al rischio di attacchi ed intercettazione dei dati, soprattutto in caso di connessione alla rete tramite Hotspot, Wifi pubblico o Bluetooth;
- la possibile compromissione di applicazioni attendibili presenti sul dispositivo a seguito di installazione di App dannose sul dispositivo stesso o a causa di notifiche push o in caso di abilitazione dei servizi di geolocalizzazione;

Per i rischi sopra esposti, l'accesso agli account di posta elettronica tramite dispositivi personali dovrà essere preventivamente autorizzato.

Il dispositivo dovrà essere custodito e utilizzato con la diligenza del buon padre di famiglia in quanto contente dati dell'Ente.

In caso di cessazione dei rapporti di lavoro, tutti i dati contenuti nei dispositivi personali dovranno essere distrutti ed eliminati.

Art. 7 – NETIQUETTE LEGATE ALLA SCRITTURA DELLE E-MAIL

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 delle regole di **netiquette**, rielaborate e adattate ai giorni nostri, 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.
- È 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. E fatto divieto partecipate 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.