COMUNE di CAVALLERMAGGIORE

(Provincia di CUNEO)

Via Roma n. 104 Telefono 0172/381055-381054 Telefax 0172/382638
e-mail segreteria@comune.cavallermaggiore.cn.it PEC protocollocavallermaggiore@actaliscertymail.it

Disciplinare interno per l'utilizzo dei sistemi, dati e strumenti informatici all'interno del Comune di Cavallermaggiore con contestuale informativa

ai sensi del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, provvedimento Garante Privacy 1.3.2007 n. 13, Statuto dei lavoratori come modificato dal Jobs act

Premessa

L'esigenza di adottare una informativa – policy aziendale per l'utilizzo dei personal computer fissi e portatili, dei dispositivi elettronici aziendali in generale (quali a titolo esemplificativo ma non esaustivo fax, fotocopiatrici, scanner, masterizzatori, telefoni fissi, cellulari aziendali, pen drive e supporti di memoria), della posta elettronica e internet (*di seguito il "Disciplinare*"), dei dati e patrimonio informativo, deriva da obblighi normativi (provvedimento del Garante Privacy n. 13 del 1.3.2007; modifiche allo Statuto dei lavoratori – D.P.R. n. 300/1970 – ad opera del c.d. Jobs act (D.Lgs. n. 151 del 14.9.2015); art. 88 del GDPR 2016/679). Il Garante ha emanato la Deliberazione n. 13 del 1° marzo 2007 "Lavoro: le linee guida del Garante per posta elettronica e internet" (reperibile presso: *http://www.garanteprivacy.it/garante/doc.jsp?ID=1387522*), con la quale ha inteso prescrivere ai datori di lavoro alcune misure per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet. Si richiama altresì la direttiva n. 2/2009 del Dipartimento della Funzione Pubblica.
Ma l'esigenza è proprio anche di sicurezza aziendale: studi resi noti hanno rilevato in Italia la presenza di un allegato o di un link malevolo in 1 email ogni 141, percentuale vicina alla media mondiale di 131: in questa "speciale" classifica l'Italia si posiziona, purtroppo, al terzo posto a livello mondiale come destinazione di attacchi (7,1%) e, in Europa, si posiziona al primo posto davanti a Paesi Bassi (3,4%), Russia e Germania (3,0%) e Regno Unito (2,7%).
Premesso che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi ai principi di diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, il disciplinare interno costituisce strumento diretto ad evitare che comportamenti anche inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati e quindi del proprio sistema informatico.
Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti i designati/incaricati in attuazione del Regolamento Europeo sulla protezione dei dati (da ora in poi GDPR 2016/679), nonché contengono le informazioni agli interessati ai sensi dell'art. 13 del GDPR 2016/679, anche in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse, come previsto dall'art. 4, comma 3° dello Statuto dei lavoratori, ad integrazione di quanto già posto in essere.
Il Titolare rende noto che il personale designato che opera all'interno dell'Ente ovvero soggetti manutentori terzi sono autorizzati a compiere, direttamente o attraverso collegamento in remoto, interventi nel sistema informatico diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, ecc.). La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività del Titolare, si applica anche in caso di assenza prolungata o impedimento dell'utente. Qualora lo specifico intervento dovesse comportare anche l'accesso a contenuti delle singole postazioni PC, il manutentore, ne darà comunicazione agli utenti interessati, preventivamente ovvero, nel caso di urgenza dell'intervento stesso, successivamente ad esso. I soggetti preposti al connesso trattamento dei dati svolgeranno solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa.

Copia del disciplinare, oltre ad essere affisso in bacheca anche per quanto prevede l'art.7 della Legge n. 300/1970, verrà consegnato a ciascun dipendente, anche ai fini dell'art. 13 del GDPR

2016/679 e dell'art. 4, comma 3°, dello Statuto dei lavoratori, e sarà messo a disposizione di amministratori, collaboratori, consulenti, tirocinanti, od altri responsabili esterni (es. incaricati software house, incaricati dei professionisti di cui si avvale il Titolare, etc.) che venissero autorizzati a far uso di strumenti tecnologici del Titolare o ad accedere alla rete informatica aziendale e ad eventuali dati ed informazioni ivi conservati e trattati.
Il contenuto del presente Disciplinare costituisce, per i dipendenti, disposizione di servizio e deve considerarsi integrativo di quanto previsto dalle informative già rese oltre che del Codice di comportamento.

Le regole che disciplinano l'utilizzo del personal computer, dei dispositivi elettronici aziendali, della posta elettronica e di internet si conformano, pertanto, ai seguenti principi generali:

- Principio di necessità (ex art. 3 Codice in materia di protezione dei dati personali): I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.
- Principio di correttezza (ex art. 11, comma 1, lett. a Codice in materia di protezione dei dati personali): Le caratteristiche essenziali del trattamento sono rese note ai lavoratori. Ciò assume particolare rilievo nel caso di trattamenti di dati acquisiti dall'elaborazione di informazioni relative alla corrispondenza elettronica, poiché un simile trattamento postula necessariamente il ricorso a tecnologie dell'informazione che, in modo più marcato rispetto ad apparecchiature tradizionali, permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa.
- Principio di determinatezza e legittimità delle finalità del trattamento (ex art. 11, comma 1 lett. b del Codice in materia di protezione dei dati personali).
- Principio di pertinenza e non eccedenza.
  Il datore di lavoro deve trattare i dati nella misura meno invasiva possibile.
- Principio di trasparenza.

Campo di applicazione del disciplinare

Il presente disciplinare si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori e consulenti del Titolare a prescindere dal rapporto contrattuale con la stessa intrattenuto (collaboratori, tirocinanti, prestatori d'opera intellettuale, etc.) che venissero autorizzati a far uso di strumenti tecnologici del Titolare o perfino di accedere alla rete informatica aziendale e ad eventuali dati ed informazioni ivi conservati e trattati.

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve così intendersi ogni dipendente, collaboratore e/o consulente (come sopra già precisato) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "Responsabile esterno del trattamento" o "terzo", ai sensi dell'art. 4 comma 10 del GDPR 2016/679, in ragione delle attività e degli impegni che si assume nell'organizzazione aziendale od a favore del Titolare stesso.

1. Utilizzo del Personal Computer e altri apparati posti a disposizione del lavoratore

1.1 Il personal computer ed eventuali altri apparati affidati all'utente (telefoni, tablet, ecc.) sono uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento. L'uso per fini personali è da considerare pertanto eccezionale e limitato a comunicazioni occasionali e di breve durata, ad esclusione dei dispositivi per i quali è esplicitamente regolamentato l'uso per fini personali.

1.2 Gli apparati dati in affidamento all'utente permettono l'accesso alla rete del Titolare solo attraverso specifiche credenziali di autenticazione.

1.3 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati né viene consentito agli

utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti, salvo quanto specificato al punto 1.5 e all'ultimo periodo del presente punto. L'inosservanza della presente disposizione espone il Titolare a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico del Titolare. Nel caso di necessità di installazione di programmi indispensabili, con scaricamento autonomo, è comunque sempre opportuno metterne al corrente l'Amministratore di Sistema.

1.4 Salvo preventiva espressa autorizzazione dell'Amministratore di Sistema, non è consentito all'utente modificare le caratteristiche impostate sugli apparati né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …).

1.5 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di Sistema nel caso in cui siano rilevati virus e adottando quanto previsto successivamente relativamente alle procedure di protezione antivirus.

1.6. Il personal computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In caso di allontanamento per breve lasso di tempo, non lasciare accessibile il personal computer: impostare un salvaschermo (screen saver) automatico protetto da password che pulisca la videata entro alcuni minuti in caso di inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

1.7 L'utente deve provvedere direttamente e personalmente al salvataggio del contenuto documentale del P.C. o altro apparato assegnato in dotazione, nell'apposita area riservata attualmente già resa disponibile sui server o Nas.

2. Gestione e assegnazione delle credenziali di autenticazione

2.1. Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dall'Amministratore di Sistema, previa formale richiesta del Responsabile dell'ufficio/settore nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.

2.2. Nel caso di soggetti "collaboratori" non dipendenti dell'Ente (*es.: tirocinanti, stagisti, LPU, ecc.*), il Responsabile dell'ufficio/settore di destinazione dovrà valutare ponderatamente e adeguatamente il tipo di profilazione ed il livello di autorizzazione all'accesso ai dati, da assegnare. Per questo tipo di profili, l'Amministratore di Sistema si riserva l'attribuzione di username che consentano di differenziare gli stessi rispetto ai profili dei dipendenti.

2.3. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (User id) associato ad una parola chiave (*password*) riservata che dovrà venir custodita dal designato con la massima diligenza e non divulgata.

2.4. La parola chiave, formata da lettere (*maiuscole o minuscole*) e/o numeri, anche in combinazione fra loro, deve essere conforme a normativa e non deve contenere riferimenti agevolmente riconducibili al designato.

2.5. È necessario procedere alla modifica della parola chiave a cura dell'utente al primo utilizzo. Successivamente, con la periodicità stabilita dall' Amministratore di Sistema, il sistema determina di default un termine di validità delle password: qualora l'utente non provveda a variare la propria password in tempo, l'accesso al personale computer, rete e/o al sistema verrà temporaneamente bloccato.

3. Utilizzo della rete informatica

3.1. Per l'accesso alla rete del Titolare ciascun utente deve utilizzare la propria credenziale di autenticazione.

3.2. È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

3.3. Le cartelle utenti presenti nei server del Titolare sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di manutenzione, amministrazione e back up da parte del dell'Amministratore di Sistema.

3.4. L'Amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza dei PC dei designati e delle unità di rete.

3.5. Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

3.6. Nella gestione dei sistemi informatici aziendali, l'Amministratore di Sistema o addetti alla manutenzione potranno acquisire informazioni generate dalle funzionalità insite negli stessi sistemi, quali, ad esempio, le informazioni sugli orari di accensione e spegnimento dei personal computer, rilevati automaticamente tramite il sistema di autenticazione al dominio di rete, e i log degli accessi a specifiche risorse di rete (file o cartelle). Tali informazioni potranno essere utilizzate per tutti i fini connessi al rapporto di lavoro, sempre nell'ambito delle finalità individuate in premessa, e con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli utenti degli stessi sistemi.

3.7. L'Ente si riserva di adottare accorgimenti correlati alla sicurezza aziendale, e in particolare: - utilizzo di sistemi e filtri che possono prevenire determinate operazioni – reputate inconferenti con l'attività lavorativa – quali l'upload o l'accesso a determinati siti e/o il download di file o software aventi particolari caratteristiche (quali ad esempio dimensionali o di tipologia di dato), con individuazione di categorie e liste di siti cui è concesso l'accesso e categorie di siti cui non è concesso l'acceso ("black lists"), in quanto non correlati con la prestazione lavorativa; - conservazione dei log di navigazione dei dipendenti per finalità di accertamento e repressione dei reati nel rispetto di quanto previsto dalla normativa vigente.

4. Utilizzo di altri dispositivi elettronici e supporti rimovibili; disciplina di altri dati inerenti il lavoratore ovvero di software o chat di messaggistica per finalità lavorative

4.1. Tutti i dispositivi elettronici e i supporti rimovibili dati in dotazione al personale devono considerarsi strumenti di lavoro, non essendo consentiti utilizzi a carattere personale o comunque non strettamente inerenti le attività lavorative. Fra i dispositivi in questione vanno annoverati i telefoni aziendali, PC portatili, tablet, chiavette USB, dischetti, CD e DVD riscrivibili, memorie esterne, ecc., indipendentemente dal fatto che l'utente abbia o meno la possibilità di accedere tramite essi alla rete del Titolare o di condividere documenti, dati e materiali ivi conservati e/o trattati.

4.2. L'utente resta responsabile nella custodia ex art 1768 cc del singolo dispositivo/supporto assegnato e deve custodirlo con diligenza sia durante trasferte e spostamenti sia durante l'utilizzo nel luogo di lavoro; va sempre adottata ogni cautela per evitare danni o sottrazioni. In caso di smarrimento o furto di dispositivi le cui memorie possano essere cancellate o bloccate da remoto a cura dell'Amministratore di Sistema per evitare sottrazioni o diffusioni di dati incontrollati, l'utente dovrà avvisare il titolare senza ingiustificato ritardo a partire dalla scoperta fatto.

4.3. I supporti magnetici contenenti dati particolari devono essere dagli utenti adeguatamente custoditi

in armadi chiusi.

4.4. L'uso di supporti rimovibili personali è consentito in caso di necessità professionale, verificandone la sicurezza.

4.5. Con riferimento ai telefoni aziendali e telefoni cellulari, fermo restando quanto sopra già disposto circa il loro uso e custodia, la ricezione o l'effettuazione di telefonate personali, così come l'invio o la ricezione di SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa, viene consentita solo nel caso di comprovata necessità ed urgenza. Inoltre, l'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile in conformità delle istruzioni al riguardo impartite dal Responsabile del servizio di appartenenza ovvero a livello generale nell'Ente.

4.6. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati particolari, ciascun utente dovrà contattare l'Amministratore di Sistema e seguire le istruzioni da questo impartite. Nel caso di dispositivi elettronici dovrà farsi particolare attenzione al salvataggio in opportuni supporti esterni di tale materiale oppure alla sua rimozione effettiva prima della riconsegna del dispositivo, concordando comunque ogni opportuna azione al riguardo con l'Amministratore di Sistema.

4.7. L'accesso ai luoghi di lavoro avviene con obbligo di timbratura mediante badge o altra modalità; i dati di accesso vengono mantenuti su appositi server e possono essere controllati dal personale autorizzato per motivi di sicurezza.

4.8. È vietato l'utilizzo dei fax dell'Ente per fini personali, tanto per spedire quanto per ricevere documentazione, l'utilizzo delle fotocopiatrici per fini personali, l'utilizzo di scanner per fini personali.

4.9. Solo in caso di eccezionale necessità e urgenza, gli Utenti possono utilizzare tali beni per motivi non attinenti l'attività lavorativa.

5. Uso della posta elettronica

5.1. La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. Il sistema di posta elettronica genera dei dati (log) indicanti il mittente, il destinatario, l'ora e la dimensione in bytes.

5.2. Al fine di garantire la continuità all'accesso dei messaggi da parte dei soggetti adibiti ad attività lavorative che richiedono la condivisione di una serie di documenti si consiglia e si incoraggia l'utilizzo abituale di caselle di posta elettronica condivise tra più lavoratori o delle caselle di posta istituzionali dell'Ente eventualmente affiancandoli a quelli individuali.

5.3. È fatto divieto di utilizzare le caselle di posta elettronica aziendale per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- L'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
- L'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- La partecipazione a catene telematiche (o c.d. "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all'Amministratore di Sistema. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

5.4 In caso di necessità e urgenza, è possibile utilizzare la Posta Elettronica per motivi non attinenti all'attività lavorativa e, comunque, non in modo ripetitivo. In tali limitati casi, le e-mail personali è opportuno che siano contrassegnate con la menzione "Privato" o "Riservato" all'inizio dell'oggetto.

5.5 Ove possibile, ai fini di una migliore differenziazione tra e-mail private o riservate ed email professionali, gli Utenti potranno chiedere ai mittenti che eventuali e sporadici messaggi privati o

riservati siano inviati con la dicitura “Privato” o “Riservato” nell’oggetto. Fermi restando i limiti generali di accesso da parte del Datore di lavoro alla posta elettronica messa a disposizione del lavoratore, all’Amministrazione non è consentito prendere visione delle e-mail che recano la menzione “Privato” o “Riservato”. In caso di controllo su base individuale e nominativa, allorché non ci sia distinzione fra Posta Elettronica privata e professionale e la natura privata di un messaggio non sia riconoscibile, l’Amministrazione presuppone che si tratti di Posta Elettronica professionale.

5.6 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili o non costituenti corrispondenza commerciale e soprattutto allegati ingombranti. In caso di cessazione del rapporto di lavoro, il singolo dipendente è tenuto ad eliminare dalle proprie cartelle tutti i messaggi di posta elettronica ed i documenti non pertinenti l’attività aziendale e non utili alle esigenze aziendali, mantenendo integra, invece, tutta la corrispondenza e documentazione inerente alla attività lavorativa. Resta inteso che, di conseguenza, la documentazione presente nel profilo del singolo utente che cessa il rapporto di lavoro verrà considerata presuntivamente dal Titolare quale corrispondenza e documentazione lavorativa e non personale.

5.7 Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

5.8 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l’Ente ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere oggetto di trattamento esclusivo del destinatario.

5.9 Poiché la casella di posta assegnata costituisce strumento di lavoro, l’uso deve essere conforme alle prescrizioni della normativa vigente.

5.9.1 È obbligatorio porre la massima attenzione nell’aprire i file attachement di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

5.9.2 Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l’accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, l’utente, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell’assegnatario della casella) imposterà l’invio automatico messaggi di risposta contenenti le coordinate di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura.

5.9.3 In caso di lunga assenza non programmata (ad es. per malattia) la procedura - qualora non possa essere attivata dal lavoratore entro due giorni avvalendosi del servizio webmail - verrà attivata a cura dell’Amministratore di Sistema.

5.9.4 Nell’ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l’ordinaria operatività aziendale sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, il dipendente può delegare a un altro dipendente a sua scelta *(“fiduciario”)* il compito di verificare il contenuto di messaggi e inoltrare al responsabile dell’area in cui lavora quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività deve essere redatto apposito verbale e informato il dipendente interessato alla prima occasione utile.

5.9.5 In caso di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l’ordinaria operatività aziendale sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, ed il dipendente non abbia delegato un suo fiduciario, secondo quanto sopra specificato, il Responsabile della struttura a cui è assegnato il dipendente può richiedere con apposita e motivata richiesta all’Amministratore di Sistema di accedere alla postazione e/o alla casella di posta elettronica del dipendente assente, in modo che si possa prendere visione delle informazioni e dei documenti necessari. Contestualmente, il responsabile della struttura deve informare il dipendente dell’avvenuto accesso appena possibile, fornendo adeguata spiegazione e redigendo apposito verbale.

5.9.6 Il Titolare si riserva la facoltà, a proprio insindacabile giudizio, di assegnare o ritirare l’utilizzo della casella di posta elettronica in base alla propria esclusiva e insindacabile valutazione della necessità di utilizzo della stessa per lo svolgimento delle attività lavorative.

5.9.7 I messaggi di posta elettronica devono contenere un avvertimento ai destinatari del seguente tenore letterale: "**Avvertenze ai sensi Regolamento Europeo 679/2016:** Le informazioni contenute in questo messaggio sono riservate, confidenziali ed a uso esclusivo del destinatario ed è vietata la loro diffusione. E' permessa una limitata comunicazione unicamente a ulteriori soggetti che possono dare un indispensabile contributo ai temi sviluppati nella mail stessa. Qualora riceveste il presente messaggio per errore e non ne siate destinatari, Vi preghiamo di darcene notizia via e-mail, di astenervi dal consultare il messaggio stesso e gli eventuali files allegati e di cancellare il messaggio dal Vs. sistema informatico. Costituisce comportamento contrario ai principi del Regolamento Europeo 679/2016 trattenere il messaggio, diffonderne il contenuto, inviarlo ad altri soggetti, copiarlo in tutto od in parte, utilizzarlo da parte di soggetti diversi dal destinatario. Comune di Cavallermaggiore garantisce la massima riservatezza dei dati da Voi comunicati; gli stessi saranno trattati in ottemperanza alle normative vigenti. L'interessato può esercitare i propri diritti di soggetto interessato dandone comunicazione all'indirizzo e-mail info@comune.cavallermaggiore.cn.it

Il Comune di Cavallermaggiore non si assume alcuna responsabilità per eventuali intercettazioni, modifiche o danneggiamenti del presente messaggio e-mail.

Information notice in accordance with General Data Protection Regulation 679/2016

The information contained in this message is confidential and for the exclusive use of the recipient. Limited communication is allowed only to subjects who can make an essential contribution to the topics provided in the email. If you receive this message by mistake and you are not a recipient, please let us know by e-mail, refrain from reading the message and opening any attached files. Please, delete the message from your system.

If you retain the message, disseminate the content, send it to other subjects, copy it whole or part of it, use it by subjects other than the recipient, you are breaking the principles of the GDPR 679/2016 Comune di Cavallermaggiore respect the utmost confidentiality of the personal information we collect from you and they will be treated in accordance with current regulations.

The person concerned can exercise his rights as interested party by giving notice to the e-mail address info@comune.cavallermaggiore.cn.it. Il Comune di Cavallermaggiore assumes no responsibility for any interception, alteration, or damage to this email."

5.9.8 La casella di posta elettronica nominativa, unitamente alle credenziali di autenticazione per l'accesso alla rete, viene disattivata al momento della conclusione del rapporto di lavoro che ne giustificava l'assegnazione. Il Titolare si riserva, tuttavia, di valutare a proprio esclusivo ed insindacabile giudizio la necessità di mantenere attiva in ricezione la casella per un congruo periodo di tempo al fine di garantire la funzionalità aziendale; in tal caso:

- Avranno accesso alla casella esclusivamente dipendenti individuati dal Titolare in funzione alle mansioni lavorative assegnate;
- Verranno inviate mail ai mittenti con indicazione della diversa casella di posta elettronica aziendale cui trasmettete i messaggi;
- La disattivazione deve essere realizzata "secondo modalità tali da inibire in via definitiva la ricezione in entrata di messaggi diretti al predetto account, nonché la conservazione degli stessi su server comunali";
- Se per esigenze lavorative così come indicato dall'Autorità Garante con il provvedimento a carattere generale del 1° marzo 2007 *"Linee guida del Garante su posta elettronica e internet"* sorge la necessità di accedere al contenuto di tale casella di posta, il responsabile della struttura organizzativa a cui il dipendente è assegnato potrà inoltrare motivata richiesta all'Amministratore di Sistema e al Responsabile di riferimento.

6. Navigazione in Internet

6. 1 Il PC o altro apparato assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.

6.2 In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:

- L'upload o il download di software anche gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato l'Amministratore di Sistema;
- L'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi autorizzati e comunque nel rispetto delle normali procedure di acquisto;
- Ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- La partecipazione a Forum non professionali, l'iscrizione con account aziendale e la partecipazione personale a social network ove non attinente all'attività lavorativa, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nickname) se non espressamente autorizzati ovvero

attinenti all'attività lavorativa.

6.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, il Titolare rende nota l'eventuale adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una "black list".

6.4 Gli eventuali controlli compiuti dal personale designato, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre tre mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza del Titolare.

6.5 L'accesso da remoto alla rete aziendale è possibile agli utenti abilitati solo a seguito di comunicazione di specifiche credenziali o dell'installazione di software che lo abilita sui dispositivi in uso.

6.6 L'accesso da remoto alla rete aziendale è possibile solo utilizzando i dispositivi previsti. A tale scopo vengono svolti controlli automatici che impediscono l'accesso utilizzando dispositivi non abilitati.

6.7 In caso di necessità e urgenza gli Utenti possono navigare in Internet per motivi non attinenti all'attività lavorativa e, comunque, non in modo ripetuto o per periodi di tempo prolungati.

6.8 È consentita la consultazione occasionale in caso di necessità ed urgenza di siti internet per finalità non istituzionali e l'accesso a caselle webmail di posta elettronica personale laddove le modalità di consultazione siano compatibili con le misure di sicurezza implementate a protezione del sistema informatico. Tale modalità non deve in ogni caso avvenire in misura pregiudizievole rispetto agli obblighi di servizio che il dipendente ha nei confronti dell'Ente.

7. Protezione antivirus

7.1 Il sistema informatico del Titolare è protetto da software antivirus aggiornato periodicamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

7. 2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto all'Amministratore di Sistema.

7. 3 Ogni dispositivo magnetico di provenienza esterna al Titolare dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato all'Amministratore di Sistema.

8. Partecipazioni a social media

8.1 L'utilizzo dei social media, dei blog e dei forum è ammissibile per attinenza alle attività professionali. L'utente deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi collaboratori, se non con il preventivo personale consenso di questi, e comunque non potrà postare sui social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro aziendali, se non con la preventiva autorizzazione del Responsabile d'ufficio.

9. Osservanza delle disposizioni in materia di privacy

9.1 L'articolo 23 del D.Lgs. 14 settembre 2015 n. 151 (così detto "Decreto sulle semplificazioni" attuativo della Legge delega 10.12.2014 n. 183, anche nota come "legge di riforma del diritto del lavoro" o "Jobs Act") ha modificato il contenuto dell'articolo 4 della Legge n. 300/1970, ora rubricato

"Impianti audiovisivi e altri strumenti di controllo".

9.2 Il testo del nuovo articolo 4 della Legge n. 300/1970, nel confermare, al primo comma, la disciplina applicabile agli strumenti di controllo a distanza dell'attività dei lavoratori necessari per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale (come le telecamere o i rilevatori di posizione Gps), che rimangono sottoposti alla stessa disciplina di divieti e di controlli di prima, ha introdotto, ai commi due e tre, una disciplina diversa per quanto concerne i dispositivi utilizzati dal lavoratore per rendere la prestazione lavorativa (computer, tablet, telefoni, smartphone) stabilendo espressamente che "La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze. Le informazioni raccolte a sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal D.Lgs. 30 giugno 2003 n. 196".

9.3 Alla luce delle disposizioni dettate dal succitato D.Lgs. n. 151/2015, l'ente può effettuare controlli sugli strumenti informatici utilizzati dal lavoratore per rendere la prestazione lavorativa (personal computer, tablet, telefoni e smartphone), senza la necessità di accordi sindacali preventivi e fornendo al lavoratore un'adeguata informativa sulle regole previste per l'utilizzo lavorativo ed eventualmente personale degli strumenti di cui si tratta e sulle modalità e i casi in cui potranno effettuarsi i controlli.

9.4 Si dà atto che l'informativa ai lavoratori, di cui al precedente capoverso, viene garantita dall'ente mediante la diffusione del presente disciplinare, e che le informazioni raccolte sono utilizzabili a tutti i fini connessi al rapporto di lavoro nel rispetto di quanto previsto dalla normativa in materia di privacy.

9. 5 Gli strumenti tecnologici considerati nel presente disciplinare costituiscono strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n. 300/1970; conseguentemente, le informazioni raccolte, possono essere utilizzate per tutti i fini connessi al rapporto di lavoro, essendo stata data, con il presente documento, informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico aziendale ovvero nel singolo strumento e sui conseguenti sistemi di controllo che potrebbero eventualmente essere compiuti, fermo restando il rispetto della normativa in materia di protezione dei dati personali (GDPR 2016/679).

9.6 Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il loro utilizzo come strumenti per il controllo a distanza dell'attività dei lavoratori; peraltro, lì dove l'adozione di tali apparati risultasse necessaria per finalità altre, es. esigenze organizzative e produttive, di sicurezza del lavoro e/o di tutela del patrimonio aziendale, il Titolare provvederà conformemente a quanto disposto dall'art.4, comma primo, della Legge n. 300/1970, dandone anche opportuna informazione agli utenti stessi.

10. Controlli e accesso ai dati trattati dall'utente

10.1 L'Ente si riserva di effettuare controlli per verificare il rispetto del Disciplinare. Rispetto a tali controlli il presente Disciplinare costituisce preventiva e completa informazione nei confronti dei dipendenti.

10.2 Gli eventuali controlli generali ed estesi atti a verificare condotte non conformi al presente Disciplinare avverranno preliminarmente su dati aggregati (*c.d. "controllo anonimo"*) riferiti all'intera struttura lavorativa ovvero al Settore o all'intero Ente, ove per caratteristiche intrinseche alla struttura organizzativa, essa non offrisse garanzie di completa anonimità della verifica. Nel caso vengano rilevate anomalie o irregolarità, potrà essere inviato un avviso generalizzato ai dipendenti che richiami questi ultimi all'utilizzo corretto degli strumenti elettronici aziendali, nel rispetto della normativa vigente e dei diritti dei terzi, con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

10.3 Qualora le anomalie o le irregolarità dovessero persistere, si procederà circoscrivendo l'invito al personale afferente all'area in cui è stata rilevata l'anomalia. In caso di ripetute anomalie o

irregolarità si procederà a controlli su base individuale, su singoli nominativi, basi e postazioni.

10.4 Qualora venga constatata la violazione del presente Disciplinare, potranno essere irrogate le sanzioni applicabili previste dai contratti collettivi vigenti, nel rispetto delle procedure stabilite dagli stessi contratti.

10.5 Oltre a ciò, l'Ente si riserva di effettuare specifici controlli sui software caricati sui personal computer utilizzati dai dipendenti al fine di verificarne la regolarità sotto il profilo delle autorizzazioni e delle licenze, nonché, in generale, la conformità degli stessi alla normativa vigente e, in particolare, alle disposizioni in materia di proprietà intellettuale.

10.6 Oltre a tali controlli di carattere generale, l'ente si riserva comunque le facoltà previste dalla normativa vigente di effettuare specifici controlli ad hoc nel caso di segnalazione di attività che hanno causato danno all'Amministrazione, che ledono diritti di terzi o che , comunque, sono illegittime.

10.7 Inoltre, si rammenta che in osservanza della vigente normativa, i dati relativi all'utilizzo della posta elettronica e di internet sono conservati per periodi di tempo strettamente limitati (non oltre un semestre). Eventuale prolungamento dei tempi di conservazione sarà valutato come eccezionale e potrà avere 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 (precontenzioso o contenzioso in atto); obbligo di custodire e/o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

10.8 Per necessità manutentive inoltre l'Amministratore di Sistema o addetti alla manutenzione potranno accedere alle dotazioni strumentali anche da remoto, con il consenso esplicito del dipendente cui la dotazione sia assegnata, mediante appositi software.

10.9 In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati. In particolare, l'Ente non utilizza sistemi hardware e software preordinati al controllo a distanza attraverso i quali sia possibile: riprodurre e memorizzare sistematicamente le pagine web visualizzate dal lavoratore; utilizzare strumenti di lettura e di registrazione dei caratteri inseriti tramite tastiera o analogo dispositivo o i movimenti del mouse; effettuare analisi occulta di computer portatili o altri dispositivi affidati in uso.

11. Sanzioni

11.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Disciplinare. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, e nei confronti dei collaboratori, consulenti, agenti ed incaricati esterni, verificata la gravità della violazione contestata, con la risoluzione od il recesso dal contratto ad essi relativo nonché con tutte le azioni civili e penali consentite.

12. Aggiornamento e revisione

12.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Disciplinare.

12.2 Il presente disciplinare/informativa è soggetto periodicamente a revisione.

12.3 Costituisce parte integrante del presente Disciplinare il provvedimento del Garante Privacy 1.3.2007 n. 13 consultabile cliccando su quanto segue: *http://www.garanteprivacy.it/garante/doc.jsp?ID=1387522*. L'utente è inoltre tenuto a verificare periodicamente eventuali aggiornamenti della disciplina in materia di dati e privacy, sul sito web dell'Ente, nell'apposita sezione dedicata.

13. Gestione degli incidenti e databreach

13. 1 Ogni incidente *(ad es. malfunzionamento PC, indisponibilità dei servizi applicativi e di rete, furto o smarrimento di dispositivi, sottrazione di dati, invio accidentale di dati all'esterno)* deve essere segnalato dall'Utente in modo tempestivo all'Amministratore di Sistema, che raccoglierà le segnalazioni e avvierà il relativo processo di classificazione e risoluzione dell'incidente medesimo al fine di minimizzare gli eventuali impatti negativi sul normale svolgimento delle attività lavorative. Nel caso l'incidente di una certa gravità riguardi il patrimonio Informativo e di conoscenza detenuto dall'Ente oppure le applicazioni informatiche, l'Utente dovrà avvisare con la massima tempestività. Per gli incidenti che possono determinare una violazione dei dati personali, cioè la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati *(cd. "databreach")* l'art. 33 del GDPR prevede che in caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il successivo art. 34 disciplina il caso in cui la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche: in tal caso è necessario comunicare la violazione all'interessato senza ingiustificato ritardo, a meno che non si verifichino le circostanze indicate nel paragrafo 3 dell'articolo:

a) il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia. Per ottemperare agli obblighi imposti dalla norma ogni Utente informa dettagliatamente l'Amministratore di Sistema o gli addetti alla manutenzione, i quali valuteranno, unitamente al DPO (Data protection officer), il prosieguo *(notifica autorità di controllo, comunicazioni all'interessato, ecc.)*.

14. Dati personali.

14.1 In questo paragrafo si vuole porre l'attenzione sugli aspetti di sicurezza relativi al trattamento di dati personali. Ai fini della corretta applicazione delle indicazioni che seguono, si ritiene utile riportare di seguito la classificazione dei dati personali fatta dal legislatore.

Ai sensi dell'Art. 4 del GDPR, è un **"dato personale"** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

I dati personali devono essere trattati e protetti secondo quanto previsto dal GDPR e dal Codice.

I dati personali, oggetto di trattamento, devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

I dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

I dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non

autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali *(«integrità e riservatezza»).*
All'atto della dismissione di supporti che contengano dati personali è necessario distruggere o rendere inutilizzabili (cancellandone il contenuto) i supporti medesimi, secondo quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008 sui "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali".

14.2 **Dati particolari/sensibili e giudiziari/ relativi a condanne penali e reati**.
Tutti gli Utenti devono porre particolare attenzione nei trattamenti dei dati personali particolari/sensibili e giudiziari/ relativi a condanne penali e reati (definiti all'art. 9 del GDPR) in relazione alla confidenzialità dei dati.
Sono indicati alcuni comportamenti o regole minime da rispettare: cifrare i dati memorizzati sui file/database o in fase di trasferimento; proteggere i canali di trasmissione; evitare l'invio con la posta elettronica di dati sensibili e giudiziari; recuperare tempestivamente i documenti stampati o ricevuti via fax che contengano dati sensibili o giudiziari per sottrarli alla vista di chi non è autorizzato; separare logicamente i dati "comuni" da quelli sensibili/giudiziari nei database, ecc.

14.3 **I dati diversi da quelli personali**
Fatto salvo il requisito dell'Integrità, i dati diversi da quelli personali sono classificati in base al livello di Confidenzialità (Confidentiality) come segue:

1. *Dati riservati*: appartengono a questa categoria i dati a cui siano collegati interessi giuridicamente rilevanti (come ad es. la proprietà individuale, il diritto d'autore e i segreti commerciali). La gestione, trasmissione e condivisione dei dati riservati deve essere sottoposta a particolari cautele e misure, stabilite dal soggetto responsabile, al fine di preservare la confidenzialità dei dati medesimi.
   L'eventuale manutenzione, effettuata da partner privati, sui sistemi ed apparati che ospitano dati riservati deve essere disciplinata, a livello contrattuale, prevedendo specifici obblighi di riservatezza a carico dei partner privati.
2. *Dati non riservati*: appartengono a questa categoria: i dati il cui accesso e/o utilizzo non ha restrizioni (ad es. gli "Open Data", i dati oggetto di "accesso civico", ecc.)
   Per i dati non riservati, vige la normativa di settore (Legge n. 241/1990, D.Lgs. n. 33/2016, ecc.).

15. Messaggistica, social network per finalità lavorative

15.1 Il contenuto del presente Disciplinare si applica anche ai servizi, software, social, di comunicazione per esigenze lavorative (*es.: Whatsapp, Telegram, ecc.),* in parte già attivati, per i quali valgono le stesse regole stabilite nel presente disciplinare per mail e navigazione su internet in ordine alle cautele di sicurezza, alla custodia, conservazione e controllo dei dati.

16. Smart working

16.1 Il Comune ha attivato e potrà ulteriormente attivare postazioni di "smart working". In tale contesto può essere implementato un sistema software che genera log, predisposto affinché sia sempre garantita la riservatezza ed evitato il controllo generalizzato a distanza del lavoratore. Ove vengano utilizzate dotazioni informative personali, l'utilizzatore deve comunque attenersi ai criteri generali di sicurezza di cui al presente disciplinare, in particolar modo per quanto riguarda l'eventuale utilizzo di reti non dedicate o non correlate ad alti profili di sicurezza (*wifi pubblici, ecc.*), in relazione alla tipologia di dati gestiti attraverso la rete.

IL SEGRETARIO COMUNALE	IL RAPPRESENTANTE DEL TITOLARE DEL TRATTAMENTO (COMUNE DI CAVALLERMAGGIORE
Paolo FLESIA CAPORGNO	*Il Sindaco - Davide SANNAZZARO*

Per ricevuta e presa visione: Il lavoratore

Lì _____ ----------

APPENDICI SUCCESSIVE:

INFORMATIVA PRIVACY

Informativa ai sensi dell'art. 13 del GDPR 2016/679

Gent. Sig./Sig.ra,
Ai sensi dell'art. 13 del GDPR 2016/679 Le forniamo le seguenti informazioni in relazione agli eventuali controlli difensivi sui luoghi di lavoro, condotti dal Comune di Cavallermaggiore sui dati generati dall'utilizzo dei sistemi e degli strumenti informatici dell'Ente.

Titolare del trattamento e Responsabile della Protezione Dati

Il Titolare del trattamento dei dati è il Comune di Cavallermaggiore, con sede in Cavallermaggiore (CN) - via Roma 104, CF/P.IVA 00330720046, PEC protocollocavallermaggiore@actaliscertymail.it, tel. +39 0172/381055 Int 3, nella persona del Sindaco pro tempore.

Il Responsabile per la Protezione dei Dati (DPO - Data Protection Officer) è TAVELLA avv. Silvio, telefono STUDIO LEGALE TAVELLA 0171/489271 Email: RPD@comune.cavallermaggiore.cn.it PEC avv.tavella@legalmail.it

1. Finalità del trattamento

I controlli condotti dall'Ente sui dati generati dall'utilizzo degli strumenti e dei sistemi informatici dello stesso sono connessi a specifiche esigenze organizzative e per finalità di accertamento e repressione degli illeciti, nel rispetto di quanto previsto dalla normativa vigente. Pertanto, la liceità del trattamento è insita nell'esecuzione dei contratti collettivi vigenti.

2. Modalità del trattamento

I dati relativi alle presenze del personale, registrati tramite sistema di timbratura vengono mantenuti su appositi server e possono essere controllati dal personale designato per motivi di sicurezza.

Gli eventuali controlli generali ed estesi atti a verificare condotte non conformi al presente Disciplinare avverranno preliminarmente su dati aggregati (c.d. "controllo anonimo") riferiti all'intera struttura lavorativa ovvero al Settore o all'intero ente, ove per caratteristiche intrinseche alla struttura organizzativa, essa non offrisse garanzie di completa anonimità della verifica. Nel caso vengano rilevate anomalie o irregolarità, potrà essere inviato un avviso generalizzato ai dipendenti che richiami questi ultimi all'utilizzo corretto degli strumenti elettronici aziendali, nel rispetto della normativa vigente e dei diritti dei terzi, con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Qualora le anomalie o le irregolarità dovessero persistere, si procederà circoscrivendo l'invito al personale afferente all'area in cui è stata rilevata l'anomalia. In caso di ripetute anomalie o irregolarità si procederà a controlli su base individuale, su singoli nominativi, basi e postazioni.

Qualora venga constatata la violazione del presente Disciplinare, potranno essere irrogate le sanzioni applicabili previste dai contratti collettivi vigenti, nel rispetto delle procedure stabilite dagli stessi contratti.

Oltre a ciò, l'ente si riserva di effettuare specifici controlli sui software caricati sui personal computer utilizzati dai dipendenti al fine di verificarne la regolarità sotto il profilo delle autorizzazioni e delle licenze, nonché, in generale, la conformità degli stessi alla normativa vigente e, in particolare, alle disposizioni in materia di proprietà intellettuale.

Gli eventuali controlli compiuti dal personale designato sulla navigazione in internet svolta dai dipendenti durante l'attività lavorativa potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta.

3. Periodo di conservazione dei dati

Il controllo sui "file di log" di cui al punto 2. non è continuativo ed i file stessi vengono conservati non oltre tre mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza del Titolare.

I dati relativi all'utilizzo della posta elettronica sono conservati per periodi di tempo strettamente limitati (non oltre un semestre). Eventuale prolungamento dei tempi di conservazione sarà valutato come eccezionale e potrà avere 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 (precontenzioso o contenzioso in atto); obbligo di custodire e/o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

4. Natura obbligatoria/facoltativa del conferimento

Il consenso non è necessario in quanto il trattamento dei dati personali così effettuato riguarda l'esecuzione del contratto di lavoro e del rispettivo contratto collettivo nazionale, in riferimento alla possibilità del datore di lavoro di irrorare sanzioni disciplinari nell'ambito del rapporto di lavoro, fatti salvi i limiti stabiliti dai contratti collettivi nazionali stessi.

5. Destinatari

I Suoi dati personali non verranno da noi diffusi, cioè non ne verrà data conoscenza a soggetti indeterminati in alcun modo, ma saranno trattati dai soli soggetti designati per le suddette finalità ed eventualmente comunicati all'Autorità giudiziaria per il perseguimento e/o prevenzione degli illeciti.

6. Trasferimento dei dati

I dati personali sono conservati su server ubicati all'interno dell'Unione Europea. Resta in ogni caso inteso che il Titolare, ove si rendesse necessario, avrà facoltà di spostare i server anche extra-UE. In tal caso, il Titolare assicura sin d'ora che il trasferimento dei dati extra-UE avverrà in conformità alle disposizioni di legge applicabili.

7. Diritti dell'interessato

L'interessato potrà esercitare i propri diritti, rivolgendo una richiesta scritta al Titolare del Trattamento e/o al Responsabile della Protezione dei dati (DPO), in quanto ai sensi dell'art. 15 del GDPR 2016/679 l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

L'interessato ha, inoltre, il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale.

Il titolare del trattamento fornisce, su richiesta, una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il diritto di ottenere una copia di cui sopra non deve ledere i diritti e le libertà altrui.

Il Titolare del trattamento
Il Sindaco

Tablet presso il Comando di Polizia Municipale

Presso il Comando della Polizia Municipale sono in uso dei tablet finalizzati al dialogo con gli archivi della Motorizzazione e del PRA. Il programma installato consente infatti di verificare, tramite l'inserimento dei dati della targa del veicolo, la regolarità dello stesso. All'applicativo accedono tutti gli agenti tramite password personalizzata e riservata. Il tablet è inoltre dotato di antivirus e di credenziali di autentificazione all'accensione; è sempre presidiato dal designato o conservato presso gli uffici del Comando, in armadio chiuso.