Città di Piazza Armerina
Libero Consorzio Comunale di Enna

# COMUNE DI PIAZZA ARMERINA



**APPROVATO CON DELIBERAZIONE DI CONSIGLIO COMUNALE N. 15 DEL 03-03-2025**

# REGOLAMENTO RELATIVO ALL'USO DELLA RETE, DEI DEVICES E DEGLI STRUMENTI ELETTRONICI

# REGOLAMENTO RELATIVO ALL'USO DELLA RETE, DEI DEVICES E DEGLI STRUMENTI ELETTRONICI

## INDICE

# REGOLAMENTO RELATIVO ALL'USO DELLA RETE, DEI DEVICES E DEGLI STRUMENTI ELETTRONICI



## 1. SCOPO

Il presente regolamento disciplina l'utilizzo degli strumenti elettronici e le modalità di accesso e di uso delle risorse informatiche, elettroniche e della rete del Comune di Piazza Amerina (d'ora in poi "Comune" o "Ente") e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire.

Il presente Regolamento definisce le regole principali da seguire durante l'uso della postazione informatica in proprio possesso.

Il presente documento è stato redatto dal Responsabile del I Settore, verificato dal Responsabile Protezione Dati (d'ora in poi "DPO") e approvato dalla Giunta Comunale e dal Consiglio Comunale.

Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere rimosse nel più breve tempo possibile.

Lo scopo del presente Regolamento è di dettare e formalizzare le linee di condotta per l'utilizzo dei Personal Computer, dei telefoni, della posta elettronica, della navigazione in Internet e della rete informatica nonché degli strumenti informatici in genere; informare preventivamente i dipendenti-utilizzatori - in ottemperanza a quanto previsto dal Regolamento Europeo 2016/679 nonché dalla legge 20 maggio 1970, n. 300 "Statuto dei lavoratori" – circa le procedure che il Titolare del Trattamento (Comune di Piazza Armerina) ha adottato in relazione al corretto utilizzo delle attrezzature informatiche ed elettroniche messe a disposizione dei propri lavoratori.

Inoltre il presente regolamento disciplina l'utilizzo della mail e della PEC istituzionale all'interno dell'Ente

## 2. PRINCIPI GENERALI

*IL COMUNE* promuove l'utilizzo della rete e dei supporti elettronici quale strumento utile per perseguire le proprie finalità e la propria azione amministrativa.

L'ambito lavorativo porta la nostra organizzazione a gestire una serie di "informazioni", proprie e dei Cittadini, per poter erogare i servizi e tutte le attività connesse all'attività dell'amministrazione dell'Ente.

Tali informazioni possono essere considerate, ai sensi del Regolamento UE 679/2016 (in seguito "GDPR"), "dati personali" quando sono riferite a persone fisiche e, per la loro gestione (trattamento), sia cartacea che digitale, è necessario che l'Ente adotti una serie di misure di sicurezza adeguate in considerazione del rischio.

Altre informazioni, pur non essendo "dati personali" ai sensi di legge, sono in tutto e per tutto "informazioni riservate", ovvero informazioni particolarmente sensibili, con particolare riferimento ai dati degli utenti che accedono ai servizi erogati, specie se questi dati contengono dati idonei a rilevare le condizioni economiche sociali o lo stato di salute degli utenti stessi, per le quali l'Ente è chiamato a garantire la riservatezza, nel rispetto della normativa vigente in materia di privacy e per la propria immagine che pone la riservatezza, l'integrità dei dati conferiti dalle terze parti alla nostra come elemento imprescindibile della nostra azione amministrativa.

Ai fini di questo Regolamento si specifica, pertanto, che con il termine "dati" deve intendersi l'insieme più ampio di informazioni di cui un dipendente o un collaboratore può venire a conoscenza e di cui deve garantire la

riservatezza e la segretezza e non solo i "dati personali" intesi a norma di legge.

Inoltre, nell'ambito della sua attività, *il COMUNE* tratta "dati cartacei" ovvero informazioni su supporto cartaceo e "dati digitali" ovvero informazioni che vengono memorizzate o semplicemente transitano attraverso apparecchiature digitali.

In linea generale, ogni dato, nell'accezione più ampia sopra descritta, di cui l'incaricato viene a conoscenza, nell'ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con l'organizzazione stessa o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita dell'Ente.

Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio i servizi erogati dall'Ente.

La progressiva diffusione delle nuove tecnologie informatiche ed in particolare l'accesso alla rete internet dal computer espone l'Ente a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine dell'organizzazione stessa.

Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, tra i quali rientrano l'utilizzo delle risorse informatiche ed elettroniche, devono sempre ispirarsi al principio di diligenza e correttezza, il *COMUNE* ha adottato il presente regolamento con l'obiettivo di evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature del *Comune.*

I dipendenti e collaboratori del *COMUNE DI PIAZZA ARMERINA* manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi di servizio e di comportamento per i dipendenti pubblici.

Consapevoli delle potenzialità offerte dagli strumenti informatici ed elettronici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.

Il presente Regolamento tiene conto del provvedimento adottato dal Garante per la protezione dei dati personali, denominato "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" – 27 novembre 2008.

Il presente regolamento integra gli obblighi in termini di riservatezza e privacy riportati nel Codice di Comportamento del Comune di Piazza Armerina di cui al D.P.R. n.62 del 2013.

## 3. POLITICHE DI SICUREZZA DEL SISTEMA INFORMATIVO

### 3.1 POLITICA DI GESTIONE DELLA SICUREZZA DEI SISTEMI

*IL COMUNE* ha deciso di porre come obiettivo principale il governo e il rispetto della sicurezza delle informazioni trattate durante l'erogazione dei

propri servizi nel rispetto dei contesti legislativi ove opera.

Sicurezza delle Informazioni all'interno dell'Ente significa assicurare:

- riservatezza: assicurare l'accesso alle informazioni solo agli autorizzati;
- integrità: assicurare che le informazioni siano complete e non modificate;
- disponibilità: assicurare che le informazioni siano accessibili agli autorizzati quando richiesto.

Il *Comune*, nell'ambito del proprio sistema di gestione dei dati e della privacy ha stabilito i propri obiettivi in materia di sicurezza dei dati e delle informazioni trattate:

- proteggere le informazioni da accessi non autorizzati, impedendo al contempo che le informazioni arrivino a non autorizzati per azioni deliberate o mancanza di cura;
- proteggere l'integrità delle informazioni salvaguardandole da modifiche non autorizzate;
- assicurare che le informazioni siano a disposizione degli autorizzati quando ne hanno bisogno;
- controllare l'evoluzione delle minacce e delle associate vulnerabilità ai sistemi informativi;
- ottemperare alle disposizioni normative e legislative in materia di trattamento dei dati;
- assicurare la continuità delle attività amministrative dell'Ente;
- formare ed addestrare il personale, promuovendo ad ogni livello un diffuso senso di responsabilità nell'utilizzo dei dati personali, con particolare riferimento ai nostri utenti,.

### 3.2 POLITICA PER L'INSERIMENTO DELL'UTENZA E PER IL CONTROLLO DEGLI ACCESSI LOGICI

A ciascun incaricato è affidato l'utilizzo e l'accesso ad un PC Client dotato di un sistema di autenticazione informatica. In particolare, è previsto l'utilizzo da parte degli Incaricati di apposite credenziali di autenticazione che consentono il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Ciascun Incaricato è reso edotto del fatto che le credenziali di autenticazione sono personali:

- devono essere memorizzate;
- non devono essere comunicate a nessuno;
- non devono essere trascritte.

Le "credenziali di autenticazione" consistono in:

- un codice per l'identificazione dell'incaricato ("user id") non assegnabile, neppure successivamente nel tempo, ad altro incaricato;

associato a,

- una parola chiave riservata conosciuta solamente dal medesimo ("password"), composta da almeno 8 (otto) caratteri (qualora il sistema preveda meno caratteri il massimo consentito), non contenente riferimenti agevolmente riconducibili all'incaricato.

Le password devono essere conformi ai requisiti di complessità:

- Non possono contenere più di due caratteri consecutivi del nome completo dell'utente o del nome dell'account utente.
- Devono includere almeno otto caratteri.

- Devono contenere caratteri appartenenti ad almeno tre delle quattro categorie seguenti:

i) Caratteri maiuscoli dell'alfabeto inglese (A-Z)
ii) Caratteri minuscoli dell'alfabeto inglese (a-z)
iii) Cifre decimali (0-9)
iv) Caratteri non alfabetici, ad esempio !, $, #, %

I requisiti di complessità vengono verificati al momento della creazione o della modifica delle password.
La password utilizzata al cambio non può essere utilizzata per i successivi 24 cambi di password.
Agli incaricati è prescritta la modifica della password almeno ogni tre mesi. Agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della password.
L'autenticazione dell'incaricato avviene tramite la verifica della "password" relativa alla "user id" associata. In particolare il sistema di password lock-out è impostato sulla base del tipo di servizio cui l'utente può accedere:

- Per quanto riguarda i servizi verso l'esterno è previsto il blocco della procedura di accesso dopo un determinato numero di tentativi falliti;
- Per quanto riguarda i servizi interni all'Ente, quindi l'accesso al dominio, dopo il terzo tentativo di accesso con una password errata, il sistema presenta un delay temporale che impedisce l'uso di attacchi brute force.

Tutti i tentativi di accesso non autorizzati sono registrati.
L'Amministratore di Sistema provvede, ogni anno, alla pulizia degli account per la disattivazione delle credenziali inutilizzate nel periodo, o riferite ad incaricati che hanno perso le qualità per accedere ai dati personali.
In caso di smarrimento della password l'incaricato deve tempestivamente richiedere una nuova assegnazione. L'Amministratore di Sistema provvede ad annullare le vecchie password e ad assegnare le nuove in via provvisoria autorizzando l'Incaricato ad inserire la propria password scelta personalmente.
In caso di necessità improrogabile, su richiesta scritta da parte del Responsabile del Settore, in qualità di delegato del Titolare del trattamento dei dati personali, ed autorizzata dal Segretario Comunale, l'Amministratore di Sistema, quale custode delle credenziali, sostituisce la parola chiave dell'incaricato con una nuova senza bisogno di conoscere la vecchia. Questa procedura garantisce l'impossibilità di collegarsi ai sistemi usando l'identità dell'incaricato senza compiere azioni che non risultino evidenti all'incaricato stesso. Infatti, al suo rientro in *Comune*, successivo ad un eventuale intervento, l'incaricato non può connettersi con la sua password, risultando quindi automaticamente avvisato dell'avvenuto intervento il quale, in ogni caso deve essere comunicato secondo quanto previsto al par. 7 del presente Regolamento.

### 3.3 POLITICA DI GESTIONE DELLE POSTAZIONI DI LAVORO

Il Personal Computer affidato all'utilizzatore è uno strumento di lavoro. L'utilizzo del medesimo per scopi non inerenti all'attività lavorativa - poiché potenzialmente idoneo ad usi impropri o illeciti come violazioni di legge, violazioni di codici di comportamento, violazioni di procedure di sicurezza o inosservanza della normativa sulla proprietà intellettuale (è vietata la copia e l'installazione di software non legalmente licenziati) - può

essere sottoposto a verifica periodica da parte dell'Ente mediante sistemi automatizzati che comunque non violino il divieto di installazione di "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (articolo, 4, primo comma, legge 300 del 1970).

La gestione della postazione di lavoro e dei devices utilizzati deve rispettare i seguenti principi:

- Il device deve essere utilizzato sempre in conformità con quanto riportato nel presente regolamento;
- Il device deve essere utilizzato in coerenza con quanto stabilito dalla normativa applicabile in materia di trattamento dei dati;
- Il device deve essere utilizzato per fini leciti e nel rispetto di quanto previsto dall'incarico al trattamento sottoscritto dagli utilizzatori
- Il device deve essere utilizzato in coerenza con le regole ed i principi etici richiamati dal *Codice di Comportamento del Comune di Piazza Armerina.*

### 3.4 POLITICA DI GESTIONE DEI CONTENUTI APPLICATIVI

*Il COMUNE* espleta la propria attività anche tramite l'ausilio di strumenti informatici e telematici e, per mere esigenze organizzative e produttive, può compiere controlli periodici a campione, riferiti a Settori e/o Servizi. o a gruppi di dati aggregati: le relative verifiche verranno comunque eseguite in conformità a quanto previsto della legge 20 maggio 1970, n. 300.

Tale attività di verifica non costituisce e non verrà utilizzata per eseguire controlli a distanza dei lavoratori, l'installazione di eventuali apparecchiature che dovessero rientrare nell'ambito di applicazione dell'art. 4 della legge 20 maggio 1970, n. 300 verrà concordata con le organizzazioni sindacali o autorizzata dall'Ispettorato del lavoro.

*Il COMUNE* informa che l'eventuale verifica sul corretto utilizzo degli strumenti informatici è volta a prevenire condotte aventi rilevanza penale, inadempimenti dell'obbligo contrattuale assunto dal lavoratore, uso improprio di attrezzatura del *Comune*, danni o modifiche nella configurazione del computer, aggravi dei costi di natura telematica (navigazione impropria su Internet).

### 3.5 POLITICA DI GESTIONE DEI CANALI DI COMUNICAZIONE

*Il COMUNE* promuove l'utilizzo della rete e dei supporti elettronici quale strumento utile per perseguire le proprie finalità. Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali.

Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.

*Il COMUNE* autorizza i lavoratori all'utilizzo degli strumenti informatici e telefonici dell'Ente, compresa i sistemi di comunicazione informatica, poiché ed in quanto necessari al corretto svolgimento delle attività lavorative.

La casella di posta, assegnata dal *COMUNE* all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse secondo quanto previsto dal presente Regolamento.

### 3.6 CLEAN DESK POLICY

Lo scopo di questa policy è quello di diffondere e rafforzare all'interno del *COMUNE* la cultura della sicurezza evitando di diffondere inavvertitamente informazioni lasciandole incustodite. Uno sforzo costante a mantenere la scrivania pulita da parte di tutti i dipendenti del *COMUNE* può notevolmente ridurre il rischio che vengano diffusi documenti cartacei contenenti informazioni sensibili sui nostri dipendenti, clienti e fornitori. Tutti i dipendenti devono familiarizzare con le linee guida contenute in questo documento.

I motivi principali di una Clean Desk Policy sono i seguenti:

- Una scrivania pulita è in grado di produrre un'immagine positiva quando i Cittadini accedono ai locali del Comune;
- Riduce il rischio di un problema di sicurezza perché le informazioni riservate non sono lasciate incustodite;
- I documenti sensibili lasciati incustoditi possono essere rubati.

Va precisato che la presente politica si applica ai seguenti documenti:

- documenti contenenti informazioni sensibili dei Cittadini e degli altri lavoratori del Comune;
- documenti contenenti informazioni sensibili per le aziende, siano esse fruitori di servizi, siano esse fornitori e consulenti dell'Ente.

Inoltre, qualora per motivi operativi non fosse possibile rispettare le indicazioni previste nella presente policy, i locali in cui documenti sono custoditi devono essere resi inaccessibili (ad es. chiusi a chiave).

Nel caso di lunghi periodi di assenza dalla scrivania, ad esempio durante una pausa pranzo, i documenti contenenti informazioni sensibili devono essere custoditi in cassetti chiusi a chiave.

Alla fine della giornata di lavoro, il lavoratore deve mettere in ordine la scrivania e rimuovere dalla scrivania tutti i documenti contenenti informazioni sensibili.

Tutti i dipendenti e collaboratori sono tenuti ad attenersi alle seguenti linee guida:

- liberare sempre l'area di lavoro prima di lasciare la scrivania per lunghi periodi di tempo;
- in caso di dubbio, dopo aver fatto una copia non autorizzata triturare o distruggere i documenti. Se non si è sicuri di essere autorizzati a duplicare della documentazione sensibile o se si è duplicata per errore, utilizzare il distruggi documenti per eliminare la copia;
- utilizzare i contenitori per lo smaltimento per i documenti riservati solo quando non sono più necessari e dopo avere usato il distruggi documenti;
- chiudere a chiave i locali, i cassetti della scrivania e gli schedari alla fine della giornata, se nei locali sono presenti documenti sensibili;
- mettere sotto chiave i dispositivi di elaborazione portatili come computer portatili o dispositivi mobili.
- trattare i dispositivi di archiviazione di massa, quali supporti rimovibili o unità USB come sensibili e riporli sempre in un cassetto chiuso a chiave.

Il dipendente che viola questa procedura può essere soggetto ad azione disciplinare.

## 4. REGOLAMENTO

### 4.1 OBBLIGHI DEL DIPENDENTE

Ogni Dipendente è tenuto a prestare la propria attività lavorativa con particolare

regolarità, diligenza e correttezza professionale, nel rispetto delle direttive impartite dai superiori e delle disposizioni di servizio, in vista degli obiettivi produttivi e di sviluppo dell'Ente (art. 2104 c.c.).

Non potrà trattare affari, per conto proprio o di terzi, in concorrenza con l'Ente a cui appartiene, né divulgare notizie attinenti all'organizzazione ed i metodi di erogazione dei servizi comunali, o comunque farne un uso tale da recare pregiudizio all'Ente.

In particolare ogni Dipendente è tenuto, per tutta la durata del rapporto di impiego, ad osservare la massima riservatezza e non potrà fornire o divulgare notizie, dati, documenti che in relazione alle mansioni affidate venissero comunque in sua conoscenza o in suo possesso.

A tal proposito Il dipendente si attiene alle seguenti regole di trattamento:

a) È vietato comunicare a soggetti non specificatamente autorizzati i dati personali, gli elementi e le informazioni dell'Ente dei quali il dipendente/collaboratore viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Ente. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio Responsabile del Settore, in qualità di delegato del Titolare del trattamento dei dati personali,;
b) È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e quant'altro;
c) È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni dell'Ente quando il dipendente/collaboratore si allontana dalla postazione di lavoro.
d) È vietato lasciare sulla postazione di lavoro (scrivania, bancone ecc.) materiali che non siano inerenti la pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di lavoratori con mansioni di front office;
e) Per le riunioni e gli incontri con utenti, cittadini, fornitori, consulenti e collaboratori dell'Ente è necessario porre particolare attenzione alla riservatezza, utilizzando apposite sale dedicate e/o evitando la presenza di soggetti non interessati.

Inoltre ogni Dipendente è obbligato a custodire e ad impiegare, con particolare diligenza, i beni comunali che gli verranno concessi in dotazione o in uso in quanto essi stessi contenenti dati personali e sensibili.

All'inizio del rapporto lavorativo o di consulenza, *Il COMUNE* valuta la presenza dei presupposti per l'autorizzazione all'uso dei vari devices, di internet e della posta elettronica da parte degli incaricati.

Successivamente e periodicamente l'Ente valuta la permanenza dei presupposti per l'utilizzo dei devices, di internet e della posta elettronica.

È fatto esplicito divieto ai soggetti non autorizzati di accedere agli strumenti informatici. I casi di esclusione possono riguardare:

- L'utilizzo di PC o di altri devices;
- L'utilizzo della posta elettronica;
- L'accesso a internet.

Le eventuali esclusioni sono strettamente connesse al principio della natura lavorativa degli strumenti informatici nonché al principio di necessità di cui al GDPR. Più

specificatamente hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo gli incaricati che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno.
I casi in cui le esclusioni dovranno risultare operative in forza di tali motivazioni verranno comunicati individualmente e potranno riguardare sia tutti i casi sopra descritti, sia solo uno o due degli stessi.
Si informa che tali esclusioni sono divenute necessarie alla luce del Provvedimento del Garante 1° marzo 2007 che indica di ridurre a titolo cautelativo e preventivo l'utilizzo degli strumenti informatici in considerazione dei pericoli e delle minacce per il nostro sistema informativo.
A seguito di una cessazione del rapporto lavorativo o di collaborazione del Dipendente/Collaboratore con l'Ente o, comunque, al venir meno, ad insindacabile giudizio del Comune, della permanenza dei presupposti per l'utilizzo dei devices, gli incaricati hanno i seguenti obblighi:

- procedere immediatamente alla restituzione dei devices, dei dati digitali e dei dati cartacei in uso;
- divieto assoluto di formattare o alterare o manomettere o distruggere i devices assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo ed i dati cartacei in suo possesso.

### 4.2 PROPRIETÀ DEGLI STRUMENTI INFORMATICI E TELEFONICI, PROGRAMMI E DATI

*IL COMUNE* è proprietario degli strumenti informatici e dei sistemi hardware utilizzati dal proprio personale per lo svolgimento delle attività e si avvale di software e di programmi antivirus di cui il *COMUNE* è unico ed esclusivo proprietario.
Per questo motivo, *Il COMUNE* è l'unico esclusivo titolare e proprietario di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri devices digitali o archiviati in modo cartaceo nei propri locali.
L'incaricato non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei devices lavorativi (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i files di filmati o altre tipologie di files) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da lui copiati, comunicati o diffusi senza l'autorizzazione dell'organizzazione.

### 4.3 AUTORIZZAZIONE ALL'UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEFONICI

*Il COMUNE* autorizza i lavoratori all'utilizzo degli strumenti informatici e telefonici di servizio, compresa la posta elettronica, poiché ed in quanto necessari al corretto svolgimento delle attività lavorative ed i servizi in Cloud per l'erogazione dei servizi offerti ai Cittadini.
Infatti, i devices assegnati sono uno strumento lavorativo nelle disponibilità dell'Incaricato esclusivamente per un fine di carattere lavorativo. I devices, quindi, non devono essere utilizzati per finalità private e diverse da quelle lavorative, se non eccezionalmente e nei limiti evidenziati dal presente Regolamento Qualsiasi eventuale tolleranza da parte del *Comune di Piazza Armerina*, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Regolamento.
L'abilitazione all'utilizzo delle attrezzature informatiche è gestita dall'Amministratore di Sistema che crea il profilo del lavoratore all'interno della nostra rete con i poteri legati

alla mansione da assolvere durante l'attività lavorativa.

### 4.4 TRASPARENZA NELLE CONDIZIONI DI UTILIZZO

L'utilizzatore è a conoscenza del fatto che le informazioni, le registrazioni e i dati trattati o memorizzati mediante i devices di servizio, inclusi i messaggi di posta elettronica inviati e ricevuti e la navigazione in Internet, non possono essere ritenuti completamente privati o confidenziali.

In relazione a tale circostanza ed al fine di evitare che si determini in capo al singolo dipendente una legittima aspettativa di riservatezza del messaggio ricevuto attraverso la posta istituzionale, si ritiene di specificare la natura "organizzativa" dello strumento informatico e dei contenuti di posta (in entrata ed in uscita) indirizzati all'indirizzo elettronico del Comune.

Conseguenza diretta di tale circostanza è che pur rimanendo le e-mail ed Internet un'area riservata dell'utilizzatore-dipendente tuttavia l'uso della posta e della strumentazione dell'Ente deve essere finalizzato al solo espletamento dell'attività lavorativa.

L'Ente, comunque, consente l'accesso e l'uso – dalla postazione di lavoro - di altro indirizzo di posta personale per l'invio di e-mail personali, purché lecite e prive di contenuti contrari all'ordine pubblico ed al buon costume secondo quanto in seguito meglio specificato. A tal fine, nel rispetto dei principi di pertinenza e non eccedenza, il Titolare può adottare, attraverso l'Amministratore di Sistema, eventuali misure che consentano la verifica di comportamenti anomali, quali un controllo preliminare dei dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Ciò al fine di evitare, da parte dell'Ente, successivi controlli specifici che realizzino un'attività di monitoraggio e controllo a distanza del lavoratore-utilizzatore.

### 4.5 CONDIZIONI DI UTILIZZO DEL PC

Il Personal Computer affidato all'utilizzatore è uno strumento di lavoro.

Il lavoratore deve accedere al dispositivo inserendo i dati del proprio profilo.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'utilizzatore con la massima diligenza e non divulgata. Nei casi di assenza dell'utilizzatore, l'accesso è altresì consentito al superiore gerarchico al fine di porre in essere gli usuali adempimenti, relativi alle normali esigenze di servizio.

Tutti i PC, compresi gli "stand alone" e i portatili, devono avere la versione più aggiornata della protezione antivirus scelta dal Comune.

Non è consentito all'utente modificare le caratteristiche di configurazione software e hardware impostate sul proprio PC, salvo previa autorizzazione scritta del Responsabile del Settore, in qualità di delegato del Titolare del trattamento dei dati personali. Qualora la richiesta è effettuata direttamente da un Dirigente responsabile del settore, la richiesta dovrà essere autorizzata dal Segretario Comunale.

Non è consentita l'installazione sul PC in dotazione di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem), se non con l'autorizzazione scritta del proprio Responsabile del Settore, in qualità di delegato del Titolare del trattamento dei dati personali,.

Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per genere, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Inoltre, nell'utilizzo dei PC, l'incaricato dovrà avere cura di:

- non lasciare accessibile il suo PC, nel caso in cui debba assentarsi dalla postazione (inserire lo screen saver o la sospensione dell'attività che rende necessaria l'autenticazione per poter riprendere l'attività lavorativa);
- non lasciare visualizzati sullo schermo, in sua assenza, dati personali;
- cancellare i dati presenti sul computer o sulla rete quando il loro mantenimento non è più necessario;
- informare il diretto superiore qualora si accorga di avere accesso a dati e programmi che non sono di sua competenza;
- non utilizzare supporti esterni con dati o programmi di provenienza ignota, per evitare infezioni da virus nel computer e di danneggiare i dati;
- chiudere sempre i programmi secondo le appropriate misure di sicurezza. Si ricorda che è assolutamente vietato collegare alla rete dell'Ente PC "esterni" (es. consulenti, clienti, fornitori etc.), se non attraverso le procedure e l'autorizzazione del proprio Responsabile del Settore, in qualità di delegato del Titolare del trattamento dei dati personali;
- nel caso ci sia la necessità di trasferire dati verso l'esterno su supporti dati, di memorizzazione o memorie di massa (USB, HDD, etc.) è fatto obbligo di utilizzare tecniche crittografiche;
- Non salvare sul CLOUD adattato dati o documenti di tipo personale.

### 4.6 INSTALLAZIONE DI PROGRAMMI SOFTWARE

L'utilizzatore non è autorizzato a scaricare, copiare o installare software; qualsiasi richiesta o esigenza in tal senso deve essere inoltrata al proprio Responsabile del Settore, in qualità di delegato del Titolare del trattamento dei dati personali,

A tal fine si ricorda a tutti gli utilizzatori che sia il software che i diritti di "copyright" sono tutelati mediante sanzioni civili e penali (D. LGS. 29 dicembre 1992, n. 518, sulla tutela giuridica del software e legge 18 agosto 2000 n, 248, contenente disposizioni in tema di tutela del diritto di autore).

*IL COMUNE* vieta tali comportamenti e non assume alcuna responsabilità riguardo a comportamenti degli utenti che possano costituire illecito, ed al contrario si rivarrà sull'utilizzatore per ogni danno o costo nel quale possa incorrere a causa di comportamenti illeciti di quest'ultimo.

È compito esclusivo dell'Amministratore di Sistema installare o far installare i software, sia di base che applicativi. L'utente non è autorizzato a cancellare dati o informazioni di proprietà dell'Ente, né a cancellare o modificare l'impostazione dei programmi installati e configurati, salvo quanto esplicitamente indicato al punto seguente o previsto dall'Amministratore di Sistema.

### 4.7 UTILIZZO DELLA POSTA ELETTRONICA ISTITUZIONALE

La casella di posta, assegnata dal *COMUNE* all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

In particolare non è consentito:

- l'utilizzo delle caselle di posta elettronica istituzionale er partecipare a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione

qualora tale uso risponda ad esigenze di lavoro;

- l'invio di messaggi di posta elettronica dal contenuto offensivo, molesto, volgare, blasfemo o comunque inappropriato;
- l'utilizzo di sistemi di posta elettronica o di strumenti informatici affidati ad altri utilizzatori, nonché l'uso di account di altri utenti;
- l'utilizzo di "anonymising remailer" o di altri sistemi per mascherare l'identità dell'utilizzatore, salvo che ciò non derivi da specifiche esigenze dell'Ente e non vi sia stata la preventiva autorizzazione scritta da parte del Responsabile del Settore, in qualità di delegato del Titolare del trattamento dei dati personali;
- l'invio di messaggi di posta elettronica tipo "catene di Sant'Antonio";
- l'utilizzo della posta elettronica per l'effettuazione di una qualsiasi attività esplicitamente vietata dal Codice di Comportamento del Comune di Piazza Armerina.

Per fini di sicurezza del sistema è obbligatorio controllare i file allegati o gli "attachments" di posta elettronica prima del loro utilizzo, ed è proibito eseguire download di file eseguibili o di documenti da siti web il cui contenuto non sia inerente la prestazione di lavoro. I documenti aventi natura confidenziale o riservata devono essere protetti da eventuali accessi di soggetti non autorizzati e non devono essere trasmessi a mezzo di posta elettronica, tranne che siano stati approntati adeguati meccanismi di sicurezza.

I messaggi di posta elettronica che costituiscono documenti lavorativi devono essere adeguatamente salvati ed archiviati nel mail server dell'Ente in modo da renderne agevole l'accesso a tutti i soggetti legittimati. Atteso che i costi associati alla conservazione di e-mail non essenziali sono notevoli, al fine di evitare la perdita delle risorse dell'Ente, l'utilizzatore, sulla base di una propria prudente valutazione, dovrà provvedere a cancellare dalla rete dell'Ente i messaggi di cui la conservazione non è necessaria.

È consentito da parte del *COMUNE* l'accesso e l'uso - dalla propria postazione lavorativa - di un indirizzo privato di posta per scopi strettamente personali ma è ribadito il divieto di utilizzazione della posta privata, il cui accesso è realizzato dalla postazione lavorativa, per finalità illecite o contrarie a norme o regolamenti.

In ogni caso l'accesso e l'uso dalla propria postazione lavorativa di un indirizzo di posta privato è consentito:

- purché l'indirizzo di posta elettronica privato non sia utilizzato per spedire o ricevere contenuti, atti, file, notizie o qualsiasi altra informazione o documento attinente all'attività lavorativa;
- purché l'accesso e l'uso dell'indirizzo di posta elettronica privato avvenga esclusivamente durante le pause regolarmente concordate con i propri Dirigenti e previste dal proprio contratto di assunzione.

### 4.8 UTILIZZO DELLA PEC

*Il COMUNE* ha attivato una PEC istituzionale. . Le credenziali di accesso alla PEC sono custodite dal Segretario Comunale.

Il Segretario Comunale è l'unico soggetto autorizzato all'invio di messaggi di posta elettronica certificata. Ogni dipendente che vuole utilizzare la PEC istituzionale per l'invio di un messaggio di posta elettronica certificata

dovrà effettuare formale richiesta di accesso alla posta elettronica al Segretario Comunale.
In caso di accettazione della richiesta di utilizzo, l'Operatore dovrà inviare via mail al proprio Responsabile del Settore, in qualità di delegato del Titolare del trattamento dei dati personali, ed al Segretario:

- il destinatario della comunicazione e l'oggetto della comunicazione
- ogni istruzione necessaria per il corretto invio del messaggio di PEC.

Per un corretto e sicuro utilizzo del servizio di posta elettronica certificata è necessario che tutti gli operatori rispettino le presenti regole:

- Non utilizzare la casella di PEC per le comunicazioni usuali (come se fosse una normale casella di posta) ma limitarne l'utilizzo alle solo comunicazioni ufficiali e per gli usi consentiti dalla legge.
- Non utilizzare la PEC se non si è ricevuta la formale autorizzazione all'invio della stessa da parte del Segretario Comunale.

*IL COMUNE* ha individuato nel I Settore la risorsa che verifica le PEC ricevute dall'Ente. Tale risorsa al fine di utilizzare correttamente la PEC deve:

- Verificare la PEC ogni qualvolta riceve una mail indicante un nuovo messaggio nella casella di PEC. In ogni caso la risorsa incaricata di verificare la PEC controlla almeno una volta alla settimana la casella di posta: i messaggi di PEC hanno validità legale e si intendono ricevuti dal destinatario nell'istante di deposito nella mailbox dell'utente, non nel momento in cui vengono effettivamente letti.
- Controllare l'occupazione della mailbox e procedere, eventualmente, ad una cancellazione dei messaggi più vecchi in modo da evitare che la casella si riempia ed i messaggi non possano essere recapitati.
- Modificare la propria password al primo accesso al servizio e successivamente secondo le regole indicate dal provider della posta elettronica.
- Adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale.

### 4.9 UTILIZZO DI INTERNET

L'accesso ad Internet e ogni simile accesso deve avvenire solo per esigenze di lavoro. È proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa. In nessun caso l'accesso ad Internet ed ogni simile accesso può essere utilizzato per:

- vedere, scaricare, ricevere o diffondere materiale pornografico, offensivo o osceno;
- compiere attività che possono essere pregiudizievoli per gli interessi dell'Ente o illegali.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto e di gestione amministrativa previste dal sistema di prevenzione della corruzione adottato.
È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
È vietata la partecipazione a forum on line non professionali, l'utilizzo di chat line (esclusi gli

strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi.

Il Comune, attraverso l'intervento dell'Amministratore di Sistema, per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'upload o il download di file, l'uso di servizi di rete con finalità ludiche o estranee comunque all'attività) adotta opportune misure che possono prevenire controlli successivi del lavoratore quali:

- la individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni – reputate inconvenienti con l'attività lavorativa – quali l'accesso a determinati siti o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato);
- trattamento di dati in forma anonima;
- eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

*IL COMUNE* è inoltre dotata di un sistema Wi-Fi a cui si accede tramite sistema di autenticazione.

### 4.10 UTILIZZO DEI PC PORTATILI

I PC portatili, come tutti gli altri strumenti di servizio, non possono essere usati per scopi diversi da quelli lavorativi.

Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni, visite, etc.), in caso di allontanamento, devono essere custoditi in un luogo adeguatamente protetto.

Nel caso di furto del PC, atteso che gli stessi contengono informazioni riservate e dati personali, si dovrà provvedere a denuncia immediata alle forze di polizia e darne immediata comunicazione al proprio Responsabile del Settore, in qualità di delegato del Titolare del trattamento dei dati personali,.

### 4.11 L'UTILIZZO DI TABLET O SMARTPHONE.

Il tablet e il cellulare (di seguito generalizzati in "device mobile") possono venire concessi in uso dall'organizzazione ai Dipendenti che durante gli spostamenti necessitino di disporre di tali strumenti e/o di connessione alla rete dell'organizzazione, per lo svolgimento della propria attività lavorativa.

Il Dipendente è responsabile dei devices mobili assegnati dall'Ente e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro e nelle sedi dove si presta l'attività lavorativa per conto del Comune.

Ai devices mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file presenti sullo stesso prima della riconsegna. In particolare i files creati o modificati sui devices mobili devono essere trasferiti sui server dell'ente prima possibile, anche on line o comunque al primo rientro in ufficio e cancellati in modo definitivo dai devices mobili (wiping) se non più necessari allo svolgimento delle mansioni assegnate. Sui devices mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dall'Ente.

I devices mobili utilizzati all'esterno (corsi di formazione, cantieri, gare, ecc…), in caso di

allontanamento, devono essere custoditi in un luogo protetto. In caso di perdita o furto dei devices mobili si deve avvisare immediatamente il proprio Responsabile del Settore, in qualità di delegato del Titolare del trattamento dei dati personali, che provvederà – se del caso – ad occuparsi delle procedure connesse alla messa in sicurezza delle informazioni e recarsi quanto prima presso le Autorità competenti di zona e dar seguito alla denuncia di smarrimento/furto. Anche di giorno, durante l'orario di lavoro, all'Incaricato non è consentito lasciare incustoditi i devices mobili assegnati.

Al Dipendente è raccomandato di assicurare la massima cautela nell'utilizzo dei devices mobili evitando, ove possibile, di lasciarli incustoditi.

I devices mobili che permettono l'attivazione di una procedura di protezione tramite digitazione di un PIN o l'uso di impronta digitale, devono sempre essere attivati attraverso l'uso di tali strumenti di protezione e non ne possono essere lasciti privi.

Laddove il device mobile sia accompagnato da un'utenza telefonica, l'Incaricato è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati, tipo di telefonate) e a rispettarli. Qualora esigenze lavorative richiedessero caratteristiche differenti l'Incaricato è tenuto ad informare tempestivamente e preventivamente il proprio Responsabile.

In relazione alle utenze mobili, salvo autorizzazione dell'organizzazione, è espressamente vietato ogni utilizzo all'estero e anche in caso di autorizzazione dell'organizzazione, gli utilizzi all'estero devono essere preventivamente comunicati all'organizzazione per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

### 4.12 MEMORIE ESTERNE (CHIAVI USB, HARD DISK, MEMORY CARD, CD-ROM, DVD, ECC.)

Agli Incaricati può essere assegnata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card, …) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. fotocamere o videocamere con memory card).

Questi dispositivi devono essere gestiti con le stesse accortezze previste per tablet e smartphone e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

Tutte le memorie esterne che contengono dati devono essere protette tramite strumenti di crittografia.

### 4.13 DEVICES PERSONALI

In generale ai dipendenti non è permesso svolgere la loro attività su PC fissi, portatili o devices personali.

Ai dipendenti, se espressamente autorizzati dall'Ente, è permesso solo l'utilizzo della posta elettronica lavorativa o applicativi di chat (es. skype) consentiti, sui loro devices personali.

In tal caso è necessario che il device abbia password di sicurezza stringenti approvate dall'Ente e l'eventuale furto o smarrimento del device deve essere immediatamente segnalato anche all'Ente per eventuali provvedimenti di sicurezza.

Al collaboratore è vietato l'utilizzo di memorie esterne personali (quali chiavi USB, memory card, fotocamere, videocamere, tablet, hard disk esterni, etc).

Gli incaricati non dipendenti (ovvero i consulenti e collaboratori esterni), possono

utilizzare i propri devices personali per memorizzare dati dell'Ente solo se espressamente autorizzati dal *Comune* stesso e assumendone formalmente e personalmente l'intera responsabilità del trattamento.
Tali devices dovranno essere preventivamente valutati dal *Comune,* per la verifica della sussistenza degli stessi livelli di sicurezza adottati all'interno dell'Ente.

### 4.14 UTILIZZO DI SISTEMI CLOUD

È vietato agli incaricati l'utilizzo di sistemi cloud non espressamente approvati dal Comune di Piazza Armerina (es. Dropbox, Google Drive.). Il *Comune di Piazza Armerina* ha attivato un servizio di Cloud Computing che consente:

- un back-up dei dati lavorati sulle singole postazioni in grado di ridurre i rischi legati allo smarrimento/furto dei dispositivi utilizzati;
- facilitare l'accesso anche da remoto (smart working) dei lavoratori;
- facilitare la condivisione delle cartelle lavorative con gli altri dipendenti di *IL COMUNE* e soggetti autorizzati, riducendo i rischi legati al trasferimento degli stessi tramite device esterni o posta elettronica.

Tutti i lavoratori dovranno svolgere la propria attività lavorativa sul Cloud.

### 4.15 PARTECIPAZIONE A SOCIAL MEDIA

L'utilizzo a fini promozionali di Facebook, Twitter, Instagram, dei blog e dei forum, anche professionali (ed altri siti o social media) è gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.

Pur garantendo il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare la propria immagine ed il patrimonio, anche immateriale, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l'orario di lavoro salvo che per il personale espressamente autorizzato.
A tal fine si richiamano le norme in materia di diritti e doveri del pubblico dipendente, con particolare riferimento al D.P.R. 16 aprile 2013 n. 62 "Codice di comportamento dei dipendenti pubblici", ed il vigente Codice di Comportamento del Comune di Piazza Armerina.
Il presente paragrafo deve essere osservato dall'utente sia che utilizzi dispositivi messi a disposizione dall'Ente, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come dipendente dell'Ente.
La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni dell'Ente, nel rispetto del segreto d'ufficio, segreto professionale e privacy.

### 4.16 AMMINISTRAZIONE TRASPARENTE E OPEN GOVERNMENT

Il Comune di Piazza Armerina riconosce ed incoraggia modalità di esercizio delle proprie funzioni basate su modelli, strumenti e tecnologie che consentono all'Amministrazione di essere "aperta" e "trasparente" nei confronti dei cittadini quale strumento di integrità e prevenzione della corruzione.
Ferme restando le disposizioni di legge in materia di trasparenza (es. Amministrazione Trasparente e/o Albo Pretorio on line)

l'incaricato dovrà porre particolare attenzione nella pubblicazione e divulgazione di documenti contenenti dati personali, facendo riferimento ai seguenti principi:

- è consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria e proporzionata alla finalità di trasparenza perseguita nel caso concreto (cd. "principi di necessità, pertinenza e non eccedenza"). Di conseguenza, i dati personali che esulano da tale finalità non devono essere inseriti negli atti e nei documenti oggetto di pubblicazione on line. In caso contrario, occorre provvedere, comunque, all'oscuramento delle informazioni che risultano eccedenti o non pertinenti;
- è, invece, sempre vietata la diffusione di dati idonei a rivelare lo "stato di salute" e "la vita sessuale o l'orientamento sessuale" (art. 9 del GDPR).

## 5. PROTEZIONE ANTIVIRUS E REGOLE PER MINIMIZZARE IL RISCHIO DI VIRUS

*IL COMUNE* impone su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente.

Il Dipendente, da parte sua, deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer, e, in particolare, deve rispettare le regole seguenti:

- Comunicare all'Amministratore di Sistema ogni anomalia o malfunzionamento del sistema antivirus;
- comunicare al proprio Responsabile del Settore, in qualità di delegato del Titolare del trattamento dei dati personali, eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, all'incaricato:

- è vietato accedere alla rete del *Comune* senza servizio antivirus attivo e aggiornato sulla propria postazione;
- è vietato ostacolare l'azione dell'antivirus installato;
- è vietato disattivare l'antivirus senza l'autorizzazione espressa dell'Ente anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer;

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico del *Comune* mediate virus o mediante ogni altro software aggressivo.

Gli utilizzatori non devono trasferire dati o programmi sul loro PC provenienti da supporti esterni (es. supporti USB, etc.) non preventivamente monitorati dall'antivirus.

L'utilizzatore che ritenga che il suo PC sia infettato da virus deve spegnere la macchina ed avvisare immediatamente il suo superiore gerarchico. Il PC potrà essere riutilizzato solo dopo che il virus sia stato rimosso su autorizzazione dell'Amministratore di Sistema.

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

- limitare lo scambio fra computer di supporti rimovibili (floppy, cd, zip) contenenti file con estensione .EXE, .COM, .OVR, .OVL, .SYS, .DOC , .XLS;
- controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta

prima di operare su uno qualsiasi dei file in esso contenuti;

- evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di "scaricare" dalla rete internet ogni sorta di file, eseguibile e non. La decisione di "scaricare" può essere presa solo dal Responsabile del trattamento;
- disattivare gli ActiveX e il download dei file per gli utenti del browser Internet Explorer;
- disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su "chiedi conferma" (il browser avvisa quando uno script cerca di eseguire qualche azione);
- attivare la protezione massima per gli utenti del programma di posta Outlook al fine di proteggersi dal codice HTML di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);
- non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");
- non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta, (in quanto potrebbe essere falso e portare a un sito-truffa);
- non utilizzare le chat;
- consultare con periodicità settimanale la sezione sicurezza del fornitore del sistema operativo e applicare le patch di sicurezza consigliate;
- seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
- avvisare l'Amministratore di Sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);
- conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);
- conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
- conservare la copia originale del sistema operativo e la copia di backup consentita per legge;
- conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

Nel caso di sistemi danneggiati seriamente da virus l'Amministratore di Sistema, procede a reinstallare il sistema operativo, i programmi applicativi ed i dati; seguendo la procedura indicata:

- formattare l'Hard Disk, definire le partizioni e reinstallare il Sistema

Operativo. (molti produttori di personal computer forniscono uno o più cd di ripristino che facilitano l'operazione);
- installare il software antivirus, verificate e installare immediatamente gli eventuali ultimi aggiornamenti;
- reinstallare i programmi applicativi a partire dai supporti originali;
- effettuare il RESTORE dei soli dati a partire da una copia di backup recente. NESSUN PROGRAMMA ESEGUIBILE DEVE ESSERE RIPRISTINATO DALLA COPIA DI BACKUP: potrebbe essere infetto;
- effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
- ricordare all'utente di prestate particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.

## 6. ASSISTENZA AGLI UTENTI E MANUTENZIONI

L'Amministratore di Sistema, può accedere ai dispositivi informatici dell'Ente sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

a) verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale;
b) verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete;
c) richieste di installazione o aggiornamento software e manutenzione preventiva hardware e software.

Gli interventi tecnici posso avvenire previo consenso dell'utente quando l'intervento stesso richiede l'accesso ad aree personali dell'utente stesso. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante credenziali utente, il personale incaricato dell'assistenza è autorizzato ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.
I dipendenti incaricati dell'assistenza informatica sono altresì autorizzati ad effettuare interventi di tipo emergenziale senza il consenso dell'utente cui la risorsa è assegnata in caso di osservazione di potenziali pericoli per i sistemi informatici dell'Ente, come, ad esempio, il rilevamento di un virus da parte del sistema antivirus centralizzato, o il rilevamento di attività di rete di tipo malevolo da parte di sistemi di intrusion detection o sulla base dell'analisi dei log del firewall.
Gli incaricati dell'intervento potranno in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza del sistema informativo e dei dati, sia sui PC assegnati agli utenti sia sulle unità di rete.
L'accesso in teleassistenza sui PC della rete dell'Ente richiesto da terzi (fornitori e/o altri) deve essere autorizzato dal Responsabile del Settore, in qualità di delegato del Titolare del trattamento dei dati personali, per le verifiche delle modalità di intervento per il primo accesso.
Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.
Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente deve presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente Regolamento.

## 7. CONTROLLI

# REGOLAMENTO RELATIVO ALL'USO DELLA RETE, DEI DEVICES E DEGLI STRUMENTI ELETTRONICI



*IL COMUNE di PIAZZA ARMERINA* espleta la propria attività anche tramite l'ausilio di strumenti informatici e telematici e, per mere esigenze organizzative e produttive, può compiere controlli periodici a campione, riferiti a singole aree produttive o a gruppi di dati aggregati: le relative verifiche verranno comunque eseguite in conformità a quanto previsto della legge 20 maggio 1970, n. 300. Tale attività di verifica non costituisce e non verrà utilizzata per eseguire controlli a distanza dei lavoratori, l'installazione di eventuali apparecchiature che dovessero rientrare nell'ambito di applicazione dell'art. 4 della legge 20 maggio 1970, n. 300 verrà concordata con le organizzazioni sindacali o autorizzata dall'Ispettorato del lavoro.

*IL COMUNE* informa che l'eventuale verifica sul corretto utilizzo degli Strumenti Informatici è volta a prevenire condotte aventi rilevanza penale, inadempimenti dell'obbligo contrattuale assunto dal lavoratore, uso improprio di attrezzatura di lavoro, danni o modifiche nella configurazione del computer, aggravi dei costi di natura telematica.

Poiché in caso di violazioni contrattuali e giuridiche, sia l'Ente, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. *Il Comune*, infatti, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, c.2), di sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. 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, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.

I controlli devono essere effettuati nel rispetto del presente Regolamento e dei seguenti principi:

- Proporzionalità: il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resterà sempre entro i limiti minimi.
- Trasparenza: l'adozione del presente Regolamento ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti.
- Pertinenza e non eccedenza: ovvero evitando un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli prolungati, costanti o indiscriminati.

L'uso degli strumenti informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'utente, possono essere oggetto di controlli da parte dell'Ente, per il tramite del personale incaricato, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, etc.). Gli interventi di controllo sono di due tipi, di seguito descritti, e possono permettere all'Ente di

prendere indirettamente cognizione dell'attività svolta con gli strumenti:

a) *Controlli per la tutela del patrimonio dell'Ente, nonché per la sicurezza e la salvaguardia del sistema informatico e per motivi tecnici e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware, etc.).*

Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli strumenti e alle risorse informatiche e relative informazioni il Responsabile del Settore, in qualità di delegato del Titolare del trattamento dei dati personali, per il tramite dell'Ufficio Informatica, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo strumento oggetto di controllo):

1) Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento;
2) Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'Ente potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni contenute negli strumenti informatici con possibilità di rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo dell'indirizzo IP dell'utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite;
3) Qualora il rischio di compromissione del sistema informativo dell'Ente sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti ai punti 1 e 2, il Responsabile di Settore, in qualità di delegato del Titolare del trattamento dei dati personali, unitamente al personale incaricato dei controlli, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

b) *Controlli per esigenze produttive e di organizzazione.*

Per esigenze produttive e di organizzazione si intendono – fra le altre – l'urgente ed improrogabile necessità di accedere a files o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un utente (quali file salvati, posta elettronica, chat, SMS, ecc.) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato.

Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni il Responsabile di Settore, in qualità di delegato del Titolare del trattamento dei dati personali, per il tramite del Servizio Trasparenza ed Integrità (in qualità di Amministratore di Sistema), si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo strumento oggetto di controllo):

1) Redazione di un atto da parte del Responsabile di Settore che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo strumento;
2) Incarico all'Amministratore di Sistema con credenziali di amministrazione ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'utente interessato, con avviso che al primo

accesso alla risorsa, lo stesso dovrà inserire nuove credenziali;

3) Redazione di un verbale che riassuma i passaggi precedenti;
4) In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro;
5) Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo EU 2016/679 "GDPR".

Tutti i controlli sopra descritti avvengono nel rispetto del principio di necessità e non eccedenza rispetto alle finalità descritte nel presente Regolamento. Dell'attività sopra descritta viene redatto verbale, sottoscritto dal Responsabile del Settore e dal Dipendente che ha svolto l'attività.

In caso di nuovo accesso da parte dell'utente allo strumento informatico oggetto di controllo, lo stesso dovrà avvenire previo rilascio di nuove credenziali (salvo diverse esigenze tecniche).

## 8. SANZIONI

Come previsto dall'art. 7 della legge 300/70, si porta a conoscenza di tutti gli utilizzatori che le prescrizioni contenute nel presente Regolamento hanno carattere vincolante per i dipendenti di *IL COMUNE* e devono essere considerate aggiuntive rispetto alle norme disciplinari già in vigore presso l'Ente. Eventuali violazioni del presente Regolamento (così come della normativa a cui lo stesso rinvia) possono avere gravi ripercussioni sull'Ente ed i suoi dipendenti e comportare, nei confronti del dipendente inadempiente, l'applicazione di sanzioni disciplinari, in conformità alle disposizioni di legge e del contratto collettivo applicabile.

Possono essere adottate misure disciplinari anche nei confronti di qualsiasi superiore che richieda o approvi tali comportamenti, ovvero sia a conoscenza degli stessi e non agisca prontamente per correggerli. I comportamenti che costituiscono violazione del presente Regolamento possono violare, nel contempo, anche disposizioni di legge tali da comportare per il dipendente inadempiente conseguenze di natura civile e penale (di carattere pecuniario o detentivo).

Ai dipendenti potrà venire richiesto di risarcire i danni derivanti dalle violazioni del presente Regolamento, sulla base delle procedure stabilite dalla normativa.

## 9. APPROVAZIONE

Il Codice è adottato da *IL COMUNE* mediante approvazione del Presidente in calce al presente documento ed è operativo dalla data riportata nel frontespizio.

## 10. PUBBLICITÀ

Il Regolamento deve essere portato a conoscenza del personale di *IL COMUNE* tramite invio in formato elettronico non modificabile a tutti i destinatari alla mail istituzionale.

Il Regolamento verrà pubblicato sulla sezione di Amministrazione Trasparente del Comune di Piazza Armerina.

I Responsabili dei Settori, in qualità di delegato del Titolare del trattamento dei dati personali all0interno dei servizi di propria competenza, si preoccupano della formazione e

dell'aggiornamento dei dipendenti assegnati alle proprie strutture in materia di sicurezza delle informazioni e privacy.