

# **COMUNE DI GAETA**

Provincia di Latina

## **DELIBERAZIONE DI GIUNTA**

N°21 del 29/01/2013

---

---

### **OGGETTO**

**Approvazione Regolamento per l'utilizzo degli strumenti informatici e dei servizi di telefonia e modalità di controllo del Comune di Gaeta. Integrazione Regolamento Uffici e Servizi.**

*L'anno duemiladodici, addì 29 del mese di **gennaio** in Gaeta e nella sede del Municipio, alle ore 16:00 e seguenti, si è riunita la Giunta Comunale.*

### **Sono intervenuti:**

			presente	assente
<i>Presidente</i>	<i>Cosmo</i>	<i>MITRANO</i>		<i>X</i>
<i>Assessore (Vice Sindaco)</i>	<i>Cristian</i>	<i>LECCESE</i>	<i>X</i>	
<i>Assessore</i>	<i>Pasquale</i>	<i>DE SIMONE</i>	<i>X</i>	
<i>Assessore</i>	<i>Antonio</i>	<i>DI BIAGIO</i>	<i>X</i>	
<i>Assessore</i>	<i>Sabina</i>	<i>MITRANO</i>	<i>X</i>	
<i>Assessore</i>	<i>Alessandro</i>	<i>VONA</i>	<i>X</i>	

*Partecipa con funzioni consultive, referenti e di assistenza il Segretario Generale Avv. Celestina Labbadia.*

### **LA GIUNTA**

● **Vista** la proposta di deliberazione in oggetto presentata dal Vice Sindaco Dott. Cristian Leccese;

P.P.: 06/1°

**Premesso che:**

- la diffusione delle tecnologie informatiche e telematiche ed il progressivo passaggio della società verso modelli di comunicazione sempre più integrati ed interconnessi, rende fondamentale per ogni realtà organizzativa e lavorativa, lo sviluppo di una cultura della sicurezza del proprio patrimonio informativo e della tutela dei diritti degli interessati;
- è dovere dell'Ente individuare il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione per il trattamento dei dati personali, nonché adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità;

**Richiamata** la propria delibera n° 507 del 06.05.1998 e successive modifiche ed integrazioni (da ultima deliberazione di Giunta Comunale n° 250 dell'11/10/2012) con cui si approvava il Regolamento sull'ordinamento degli uffici e servizi;

**Ritenuto** che l'elevato uso della tecnologia informatica (e in particolare l'accesso alla rete informatica e telematica, Internet e posta elettronica) come strumento di lavoro in questo Comune, impone la necessità di regolamentarne l'utilizzo, allo scopo di fornire agli utenti, (dipendenti, amministratori e collaboratori) adeguata informazione circa le modalità da seguire per un corretto utilizzo degli strumenti e delle risorse informatiche e telematiche messe loro a disposizione per lo svolgimento delle proprie mansioni istituzionali, in modo che possano collaborare alle politiche di sicurezza messe in atto;

**Ritenuto** inoltre di porre in essere adeguati e commisurati sistemi di controllo sul corretto utilizzo degli strumenti e delle risorse informatiche e telematiche, senza che ciò possa in alcun modo invadere e violare la sfera personale del lavoratore e quindi il suo diritto alla riservatezza ed alla dignità come sancito dallo Statuto dei Lavoratori e dal DLgs. 196/03;

**Richiamata** la deliberazione dell'autorità Garante per la protezione dei dati personali (G.U. del 10/03/2007) sono state definite le "linee guida del Garante per la posta elettronica ed Internet";

**Dato atto** che l'allegato Regolamento, disciplinando l'attività dei dipendenti, va comunicato alle OO.SS. in quanto interviene nell'integrazione del vigente Regolamento Uffici e Servizi;

**Visto** l'allegato "Regolamento per l'utilizzo degli strumenti informatici e dei servizi di telefonia e modalità di controllo del comune di Gaeta", che si allega alla presente deliberazione per farne parte integrante e sostanziale;

**Precisato** che tale regolamento:

- si conforma alle indicazioni fornite dal Garante per la Protezione dei dati personali che, con deliberazione n° 13 del 1 marzo 2007, ha emanato le linee guida in materia di utilizzo di strumenti informatici e telematici, nonché della posta elettronica e della rete Internet, nel rapporto di lavoro, oltre alla normativa in vigore;
- si configura come strumento a tutela dei diritti patrimoniali dell'Ente ed a garanzia della sicurezza ed integrità del proprio patrimonio informativo;

- si caratterizza come strumento di garanzia a favore di tutti coloro che svolgono un rapporto di lavoro o di servizio a beneficio dell'Ente, nella misura in cui costituisce una informativa preventiva, fornita a tutti questi soggetti, circa termini, casi e modalità di verifica del corretto utilizzo degli strumenti informatici e telematici messi a loro disposizione per le attività di lavoro o di servizio;

**Considerato** che il regolamento in parola è semplicemente attuativo della vigente normativa in parola e che si configura semplicemente come un più articolato recepimento attuativo;

**Ritenuto** di adottare l'allegato "Regolamento per l'utilizzo degli strumenti informatici e dei servizi di telefonia e modalità di controllo del comune di Gaeta", dando atto che lo stesso dovrà essere reso noto a tutti i dipendenti con le forme più efficaci ed immediate;

**Visto** lo Statuto Comunale;

**Visto** il Decreto Legislativo 18 agosto 2000, n°267 "Testo unico delle leggi sull'ordinamento degli enti locali";

**Acquisito** il parere favorevole di regolarità tecnica da parte del Dirigente del I° Dipartimento, ai sensi dell'articolo 49 - 1° comma - del Decreto Legislativo 18/08/2000, n°267;

**Dato atto** che per il presente provvedimento non è dovuto il parere di regolarità contabile;

Con votazione unanime favorevole, palesemente resa per alzata di mano

#### **D E L I B E R A**

**A** - Di approvare per le motivazioni espresse in premessa il Regolamento per l'utilizzo degli strumenti informatici e dei servizi di telefonia e modalità di controllo del comune di Gaeta che consta di n°32 articoli, il quale allegato al presente atto ne costituisce parte integrante e sostanziale.

**B** - Di dare atto che il presente Regolamento è integrazione del vigente Regolamento Uffici e Servizi di cui ne costituisce allegato integrante e sostanziale;

**C** - Di comunicare la presente deliberazione alle OO.SS.

Successivamente

#### **LA GIUNTA COMUNALE**

Ravvisata la necessità di dare immediata attuazione al presente deliberato;

Visto l'art.134 - comma 4 - del Decreto Legislativo 18/08/2000 n°267;

Previa separata votazione unanime favorevole, palesemente resa per alzata di mano,

#### **D I C H I A R A**

il presente atto **immediatamente eseguibile**.

Il presente verbale viene letto, confermato e sottoscritto nelle forme di legge.

IL VICE SINDACO

DOTT. CRISTIAN LECCESE

IL SEGRETARIO GENERALE

AVV. CELESTINA LABBADIA



**COMUNE DI GAETA**  
(Provincia di Latina)

\* \* \* \* \*

**REGOLAMENTO**

comunale per l'utilizzo degli strumenti  
informatici e dei servizi di telefonia e modalità di  
controllo del Comune di Gaeta.

\* \* \* \* \*

(Approvato con deliberazione della Giunta Comunale n°21 del 29/01/2013)

# **CAPO I**

## **Finalita' - Ambito Di Applicazione - Principi Generali**

\* \* \* \* \*

### **Articolo 1 - Finalità**

1. Il presente regolamento è diretto a definire le modalità di accesso ed utilizzo degli strumenti informatici, di internet, della posta elettronica, e dei servizi di telefonia, nell'ambito dello svolgimento delle proprie mansioni e compiti, ai fini di un corretto utilizzo degli strumenti stessi da parte degli amministratori, dipendenti e collaboratori del Comune di Gaeta.
2. L'Amministrazione promuove ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati di proprietà del Comune e disciplina le modalità con cui effettuerà i relativi controlli.

### **Articolo 2 - Ambito di applicazione**

1. Gli strumenti informatici sono costituiti dall'insieme delle risorse informatiche comunali, ovvero dalle risorse infrastrutturali e dal patrimonio informativo digitale. Le risorse infrastrutturali sono costituite dalle componenti hardware e software. Il patrimonio informativo è l'insieme delle banche dati in formato digitale ed in generale di tutti i documenti prodotti tramite l'utilizzo delle risorse infrastrutturali.
2. I servizi di telefonia sono costituiti dall'insieme delle infrastrutture telefoniche in dotazione, in particolare dalle linee e dagli apparecchi telefonici.
3. Il presente regolamento si applica a tutti gli utenti interni ed esterni. Per utenti interni si intendono gli amministratori, i dirigenti, i dipendenti a tempo indeterminato e determinato, i collaboratori coordinati e continuativi ed il personale con altre forme di rapporto di lavoro. Per utenti esterni si intendono tutti i soggetti che usufruiscono dei sistemi informativi e dei servizi di telefonia comunali per erogare un servizio pubblico (ad esempio, consultazioni anagrafiche).
4. Il presente regolamento per l'utilizzo degli strumenti informatici e dei servizi di telefonia e modalità di controllo è consegnato agli utenti interni di cui al comma 3, che lo sottoscrivono per presa visione e accettazione, quale parte integrante del contratto di lavoro o altra forma di collaborazione, (cfr. art. 30).

### **Articolo 3 - Principi generali**

1. Il Comune di Gaeta promuove l'utilizzo degli strumenti informatici, di internet e della posta elettronica quali mezzi utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali, in accordo con le linee guida e i principi delineati dalla normativa vigente.
2. Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche e telefoniche, con particolare riferimento ai servizi, ai programmi a cui ha accesso e ai dati trattati a fini istituzionali. È altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali. Sono vietati comportamenti che possono creare un danno, anche di immagine, all'Ente.
3. Ogni utente deve attenersi, nell'utilizzo degli strumenti, ai principi e ai doveri stabiliti nelle normative di riferimento; inoltre è responsabile della propria postazione di lavoro.

#### **Articolo 4 - Titolarità**

1. Il Sindaco è titolare di tutte le risorse hardware e software messe a disposizione attraverso il sistema informativo comunale.

#### **Articolo 5 - Ruoli**

1. I ruoli previsti nel sistema informativo comunale (SIC) sono i seguenti:
  - a) Titolare
  - b) Dirigente del SIC
  - c) Amministratore di sistema
  - d) Dirigenti
  - e) Personale del settore CED
  - f) Utenti
  - Al **Titolare** competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati e agli strumenti utilizzati. Il titolare è il Sindaco del Comune di Gaeta (oppure) un suo delegato.
  - Il **Dirigente del SIC**, di concerto con l'amministrazione comunale, traccia le linee generali del funzionamento di tutti gli uffici del Comune collegati al sistema informativo comunale. Compete al Dirigente del SIC la scelta del "sistema" software da adottare, di concerto con le linee stabilite dall'amministrazione comunale. Il Dirigente del SIC è anche custode della password dell'interno Sistema Informativo Comunale.
  - Dirigente del Sistema Informativo Comunale è il responsabile unico dell'intero sistema. Spetta al Dirigente del SIC l'intera gestione delle linee programmatiche stabilite dall'amministrazione del Comune di Gaeta. Faranno capo a questa figura tutti gli utenti del SI, i consulenti esterni e l'ufficio unico degli acquisti.
  - L'**amministratore di sistema** è tenuto a:

- a. elaborare e stabilire le regole per un utilizzo ragionevolmente sicuro del sistema informativo comunale, in attuazione delle direttive del Dirigente del SIC;
  - b. rendere operative, mediante il personale del settore elaborazione dati e/o di personale incaricato interno/esterno, le regole di sicurezza sul sistema informativo comunale;
  - c. controllare i sistemi, con l'ausilio del personale del settore elaborazione dati e/o di personale incaricato interno/esterno, per individuare un eventuale uso scorretto, nel rispetto della privacy degli utenti;
  - d. segnalare prontamente al Sindaco, all'Assessore all'Informatica ed al Segretario Generale ogni eventuale attività non autorizzata sul sistema informativo comunale.
- L'amministratore di sistema deve conoscere la normativa sulla privacy e deve predisporre sistemi idonei alla registrazione degli accessi logici; le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste (non sono ammesse descrizioni abbreviate). Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.
- **I dirigenti** sono tenuti a:
    - a. informare i dipendenti sull'uso appropriato delle dotazioni informatiche messe a disposizione;
    - b. informare il personale dipendente e/o assimilato sulle disposizioni in merito all'uso consentito delle risorse del sistema informativo comunale;
    - c. verificare che il personale loro assegnato si uniformi alle regole ed alle procedure descritte nel presente regolamento;
    - d. verificare che i fornitori e/o il personale incaricato esterno si uniformino alle regole ed alle procedure descritte nel presente regolamento;
    - e. adempiere a tutti gli obblighi inerenti la responsabilità in materia di trattamento di dati personali e sensibili;
    - f. accertarsi della corretta registrazione degli accessi effettuati dagli utenti del servizio pubblico di consultazione Internet, nei settori dove è erogato tale servizio;
    - g. segnalare prontamente all'amministratore di sistema ogni eventuale attività non autorizzata sul sistema informativo comunale.
  - **Il personale del settore elaborazione dati e il personale esterno** incaricato che concorre alla gestione/implementazione del sistema informativo dell'ente è tenuto a:
    - a. garantire la massima riservatezza sulle informazioni acquisite direttamente o indirettamente nell'esercizio delle proprie funzioni;
    - b. segnalare prontamente all'amministratore di sistema ogni eventuale attività non autorizzata sul sistema informativo comunale.
    - c. i compiti specifici del settore elaborazione dati o di eventuale incarico esterno sono specificatamente precisati nel contratto di fornitura o nella determinazione di incarico. È tenuto a fornire i servizi di assistenza hardware e sistemistici nei modi e nei tempi previsti dall'incarico.
  - **Gli utenti** sono responsabili per ciò che concerne:
    - a. il rispetto delle regole per l'uso consentito del sistema informativo comunale;



- b. ogni uso che venga fatto delle credenziali di autenticazione assegnate secondo le modalità indicate nell'Art. 6;
- c. la pronta segnalazione al competente dirigente di ogni eventuale attività non autorizzata sul sistema informativo comunale di cui vengano a conoscenza per motivo di ufficio.

## **Articolo 6 - Autorizzazioni**

1. Le autorizzazioni all'accesso al sistema informativo sono assegnate in funzione del ruolo di ogni utente, della collocazione di ogni dipendente comunale nell'organigramma dell'ente e delle esigenze operative comunicate preventivamente al Dirigente del SIC .
2. Il personale delle società ospitate nei locali dell'ente, delle forze di polizia, di altri enti pubblici o di società esterne può accedere ai servizi del sistema informativo comunale previo regolare permesso di accesso e richiesta documentata. Le richieste di autorizzazione all'accesso devono essere trasmesse dai responsabili delle strutture esterne al Dirigente del SIC.
3. Il personale esterno incaricato dall'ente (es. consulenti, stagisti, personale interinale) può accedere ai servizi del sistema informativo comunale nei locali dell'ente. Le richieste di autorizzazione all'accesso devono essere trasmesse dal competente dirigente all'amministratore di sistema. Il personale esterno incaricato e autorizzato dall'ente è a tutti gli effetti un utente del sistema informativo comunale ed è soggetto al presente regolamento.
4. Tutti gli utenti devono prendere visione ed accettare i termini del presente regolamento tramite la sottoscrizione del *“Modulo di presa visione ed accettazione del regolamento”*, allegato al presente regolamento.
5. Per tutte le richieste deve essere utilizzato il *“Modulo di richiesta di accesso”*, allegato al presente regolamento. Il Dirigente del SIC autorizza l'amministratore di sistema, viste le informazioni inerenti gli utenti, ad assegnare, sospendere o revocare le autorizzazioni all'accesso ai servizi hardware e software erogati dal sistema informativo attraverso le reti Intranet/Extranet/Internet.
6. Le autorizzazioni all'accesso ai servizi erogati dal sistema informativo comunale sono fornite agli utenti sotto forma di credenziali di autenticazione costituite da un nome utente e da una password.
7. Il Dirigente del SIC, su disposizione del Sindaco, redigerà due distinti documenti:
  - a) Schema dei diritti
  - b) Schema degli accessiLo schema dei diritti conterrà i singoli permessi concessi ad ogni utente con l'individuazione dei livelli concessi (lettura o scrittura, su quale archivio e per quali finalità);  
Lo schema degli accessi conterrà i singoli permessi concessi ad ogni singolo utente per l'accesso ai servizi esterni al Comune (CNSD, Agenzia delle Entrate, Internet, etc).

## **Art. 7 - Accesso ai servizi online**

1. Il Dirigente del SIC adotterà scelte tecniche affinché i software applicativi dei servizi demografici e dei tributi elaborino automaticamente credenziali di accesso per ogni cittadino ed impresa per l'accesso ai servizi online offerti dal Comune di Gaeta.
2. I cittadini che accedono ai servizi online offerti dal Comune sono a tutti gli effetti utenti del sistema informativo comunale e sono soggetti all'osservanza del presente regolamento.
3. Il Dirigente del SIC stabilirà, di concerto con il titolare, i modi per la consegna delle credenziali di accesso ai cittadini/impresae per l'accesso ai servizi online.

## **Art. 8 - Responsabilità**

1. L'utente è informato del fatto che la conoscenza delle credenziali di autenticazione da parte di terzi consentirebbe a questi ultimi l'utilizzo del sistema informativo e dei servizi erogati attraverso di esso. L'utente si impegna a non rivelare ad alcuno le proprie credenziali di autenticazione per l'accesso al sistema informativo.
2. L'utente è il solo ed unico responsabile della conservazione e della riservatezza delle proprie credenziali di autenticazione e, conseguentemente, rimane il solo ed unico responsabile per tutti gli usi ad essa connessi o correlati (ivi compresi danni e conseguenze pregiudizievoli arrecati all'ente e/o a terzi) siano dal medesimo utente autorizzati ovvero non autorizzati.
3. L'utente si impegna a comunicare immediatamente all'amministratore di sistema l'eventuale furto, smarrimento o perdita della password. In particolare, in caso di furto, l'utente si impegna a modificare tempestivamente tale password utilizzando le procedure automatiche a sua disposizione. Fino alla comunicazione scritta all'amministratore di sistema l'utente sarà responsabile delle conseguenze derivanti dal furto, dalla perdita o dallo smarrimento di tale password.
4. L'Amministratore del Sistema, su disposizione del Dirigente SIC, può cambiare le credenziali di accesso di un utente per effettuare un accesso ai dati o alle risorse hardware in dotazione, nel caso di una sua prolungata assenza o impedimento e nei casi in cui l'intervento sia indispensabile ed indifferibile per operatività e sicurezza del sistema.
5. Le credenziali di un utente vengono disattivate dall'Amministratore del Sistema, su disposizione del Dirigente SIC, nel caso in cui egli perda le qualità che gli consentono l'accesso alle risorse del sistema informativo comunale ed in ogni caso automaticamente entro sei mesi di mancato utilizzo.

## CAPO II: Criteri di utilizzo degli strumenti informatici, di internet e della posta elettronica

\* \* \* \* \*

### Articolo 9 - Modalità di utilizzo degli strumenti informatici

1. Durante l'espletamento della propria attività lavorativa, i dipendenti devono attenersi alle seguenti istruzioni e raccomandazioni:
  - a. per evitare il grave pericolo di introdurre virus informatici nei sistemi comunali, devono essere utilizzati esclusivamente programmi distribuiti dall'ente; in particolare è vietato scaricare files e software anche gratuiti, prelevati da siti internet, se non su espressa autorizzazione del Dirigente del SIC, di concerto con l'Amministratore di Sistema;
  - b. non è consentito modificare la configurazione impostata sul proprio PC e installare periferiche (hard-disk, DVD, fotocamere, apparati multimediali, ecc...) esterne agli strumenti in dotazione se non per esigenze di servizio, autorizzate dal Dirigente del SIC;
  - c. al fine di evitare di introdurre virus, è vietato copiare files di provenienza incerta da supporti quali pen drive, Cd-ROM, DVD, ecc... per finalità non attinenti alla propria prestazione lavorativa;
  - d. gli applicativi gestionali (Iride, Anagrafe, ecc...) sono destinati alla gestione di informazioni il cui utilizzo deve essere compatibile con la normativa vigente relativa alla privacy (vedi Decreto Legislativo 196/2003 e successive modificazioni);
  - e. non è consentita la consultazione, memorizzazione e diffusione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
  - f. è vietata l'installazione non autorizzata di modem che sfruttino il sistema di comunicazione telefonico per l'accesso a internet o a banche dati esterne.
  - g. non è consentito agli utenti duplicare e/o cedere programmi e altro materiale informatico, se non nelle forme e per gli scopi di servizio per i quali sono stati assegnati;
  - h. l'eventuale malfunzionamento o danneggiamento del personal computer deve essere tempestivamente comunicato al SIC tramite Service Desk.
  - i. i sistemisti ed i tecnici che hanno in gestione e seguono la manutenzione dei componenti del sistema informatico comunale possono procedere alla rimozione dei files o applicazioni che riterranno essere pericolosi per la sicurezza sia sui singoli personal computer, sia sulle unità di rete.
  - j. i sistemisti ed i tecnici del SIC incaricati della gestione e della manutenzione dei componenti del sistema informatico comunale possono, in qualsiasi momento, accedere al personal computer (anche con strumenti di supporto, assistenza e diagnostica remota) per manutenzione preventiva e correttiva, previa autorizzazione dell'utente.
  - k. ogni dipendente che dovrà per qualsiasi motivo lasciare incustodita la propria postazione di lavoro sarà tenuto a chiudere tutte le applicazioni attive e bloccare

l'accesso o spegnere fisicamente il computer (ad esempio, mediante l'utilizzo di salvaschermo dotato di password o eventuale estrazione e custodia dell'hardware di autenticazione e degli altri supporti removibili).

#### **Articolo 10 - Gestione delle password e degli account**

1. L'account è costituito da un codice identificativo personale (username o user id) e da una parola chiave (password).
2. Si distinguono account di accesso alla rete e di accesso ai programmi autorizzati, ciascuno con una specifica password, in particolare:
  - password di rete, per l'avvio e l'utilizzo del sistema operativo e di tutte le risorse di rete;
  - password per l'accesso a particolari programmi e applicativi, ivi compresa la intranet.Non è consentita l'attivazione della password di accensione (bios) del personal computer.
3. La password non deve contenere riferimenti agevolmente riconducibili all'utente. Essa deve essere modificata al primo utilizzo e periodicamente ai sensi della normativa in vigore, secondo la procedura di modifica proposta automaticamente all'utente.
4. Le password saranno di due tipologie:
  - a. pwd del sistema (server, switch, router, connessioni, etc) che dovranno essere tutte nella disponibilità del dirigente del SIC e dell'amministratore di sistema;
  - b. le pwd individuali (accesso al singolo PC, caselle di posta, PEC, firma digitale, procedure software, etc...) dovranno essere comunicate singolarmente in busta chiusa e sigillata, consegnata al "custode" delle password. Ogni utilizzatore del sistema rimane responsabile civilmente e penalmente della custodia e della segretezza delle proprie credenziali (v. Decreto Legislativo 196/2003 e s.m.i).
5. L'amministrazione provvede a nominare il "custode" delle password che può coincidere con il Dirigente del SIC, che dovrà custodire tutte le password chiuse in buste sigillate in modo sicuro. Il Dirigente del SIC, su disposizione del Sindaco, può procedere ad aprire le buste con le pwd individuali.
6. In caso di cessazione del rapporto di lavoro, l'account individuale del dipendente verrà immediatamente dismesso.
7. È compito del Servizio Personale di aggiornare tempestivamente le variazioni del personale, in modo che il Dirigente del SIC possa predisporre la creazione, modifica e/o cancellazione degli account.

#### **Articolo 11 - Utilizzo di personal computer portatili**

1. I Dirigenti, qualora ritengano necessaria l'assegnazione di personal computer portatili ad uso del proprio personale, dovranno inoltrare apposita richiesta motivata al SIC. In

linea di massima, l'assegnazione del personal computer portatile prevede la restituzione di quello fisso e l'installazione di tastiera, mouse e monitor per facilitarne l'utilizzo nella propria postazione.

2. Il Dirigente di area vigila sul corretto utilizzo del personal computer portatile e ne è corresponsabile assieme al lavoratore che deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
3. L'utilizzo del personal computer portatile è soggetto alle stesse regole previste per i personal computer fissi connessi in rete; non è pertanto cedibile a terzi estranei all'Ente e deve essere utilizzato ai soli fini istituzionali.

#### **Articolo 12 - Utilizzo delle stampanti e dei materiali di consumo**

1. L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, supporti magnetici, supporti digitali) è riservato esclusivamente ai compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

#### **Articolo 13 - Utilizzo delle periferiche e delle cartelle condivise**

1. Per periferica condivisa si intende stampante, scanner, plotter o qualsiasi altro dispositivo elettronico che può essere utilizzato in contemporanea da più uffici.
2. Per cartella condivisa (unità di rete) si intende uno spazio disco disponibile sui server centrali, per la memorizzazione di dati e programmi accessibili ad un gruppo di utenti preventivamente autorizzati.
3. L'utente è tenuto ad utilizzare le unità di rete per la condivisione di informazioni strettamente professionali; non può pertanto collocare, anche temporaneamente, in queste aree qualsiasi file che non sia attinente allo svolgimento dell'attività lavorativa. L'utente è tenuto, altresì, alla periodica (almeno ogni 6 mesi) pulizia di tutti gli spazi assegnati, con cancellazione dei files obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati al fine di evitare, salvo casi eccezionali, un'archiviazione superflua.
4. L'utilizzo delle periferiche condivise è riservato esclusivamente ai compiti di natura strettamente istituzionale.
5. I Dirigenti si impegnano ad eliminare, ove è possibile, personal computer, server, stampanti e/o gli scanner personali in favore di quelli di rete (condivisi), che permettono un risparmio nei costi di gestione.

#### **Articolo 14 - Rispetto della proprietà intellettuale e delle licenze**

1. Tutto il software in uso nel sistema informativo comunale in cui sia prevista una licenza d'uso deve essere ottenuto seguendo le procedure di acquisizione definite dal settore elaborazione dati e deve essere registrato a nome dell'amministrazione comunale.
2. Tutto il software che non richieda una licenza d'uso a titolo oneroso, quale il software a sorgente aperto (open source) o il software distribuito con licenza d'uso di tipo freeware o shareware, deve essere selezionato e reso disponibile agli utenti dal settore elaborazione dati, competente per la materia.
3. Non è possibile installare, duplicare o utilizzare software acquisiti al di fuori di quanto consentito dagli accordi di licenza.
4. Tutti gli utenti sono tenuti al rispetto delle leggi in materia di tutela della proprietà intellettuale (copyright).
5. Il Comune di Gaeta si doterà solo ed esclusivamente di software con licenza d'uso ceduta a tempo indeterminato. Tale vincolo permane anche se si adottano procedure web based, o in tecnologia ASP, o in outsourcing: rimane ferma la cautela di avere la disponibilità a tempo indeterminato delle licenze d'uso di tutti i software applicativi utilizzati. Sono esclusi da tale obbligo i sistemi operativi in caso di noleggio delle apparecchiature.
6. Le procedure software vanno installate su disposizione ed indicazioni del Dirigente del SIC; i permessi di accesso ed i diversi livelli sono stabiliti dal Dirigente del SIC in ottemperanza al seguente regolamento.

#### **Articolo 15 - Utilizzo del Software sviluppato dagli utenti**

1. I dipendenti comunali possono realizzare procedure software basate sugli strumenti di automazione messi a disposizione dagli applicativi installati a bordo delle stazioni di lavoro, utilizzando strumenti software, previa autorizzazione del dirigente del SIC, sentito il parere dell'amministratore del sistema.
2. Le procedure software realizzate devono soddisfare particolari esigenze d'ufficio, non risolvibili ricorrendo agli applicativi resi disponibili dall'ente.
3. L'utente realizzatore delle procedure software è il diretto responsabile della loro manutenzione e della integrità degli archivi gestiti.
4. Il personale del settore elaborazione dati fornisce l'assistenza necessaria a garantire il funzionamento degli ambienti di sviluppo (es. Visual Basic for Application), ma non è tenuto a fornire assistenza sul software realizzato dagli utenti.
5. Il personale del settore elaborazione dati, avvalendosi di procedure automatiche o manuali, può provvedere all'aggiornamento degli ambienti di sviluppo, senza necessità di preavviso agli utenti.

## **Articolo 16 - Utilizzo di hardware di proprietà personale**

1. L'utente può connettere postazioni di lavoro o apparati personali alle reti Intranet ed Extranet dell'ente, solo con l'autorizzazione scritta dell'amministratore di sistema.
2. L'utente può utilizzare dispositivi non autorizzati dall'amministratore di sistema per accedere ai soli servizi del sistema informativo erogati via Internet.
3. L'autorizzazione rilasciata dall'amministrazione di sistema indicherà le principali caratteristiche tecniche atte ad individuare univocamente l'hardware di proprietà personale connesso alla rete, la durata dell'autorizzazione ed il titolare delle credenziali di accesso rilasciate.
4. L'hardware sarà connesso alla rete e configurato a cura del settore elaborazione dati o di personale interno/esterno incaricato dal settore elaborazione dati. Nel caso in cui l'hardware di proprietà personale non sia dotato di un software antivirus regolarmente aggiornato, sarà negato l'accesso alla rete.

## **Articolo 17 - Utilizzo di software di proprietà personale**

1. L'utente può utilizzare software di proprietà personale, con l'autorizzazione scritta dell'amministratore di sistema, per fini esclusivi di connessione di dispositivi hardware di proprietà personale alle postazioni di lavoro.
2. Il software verrà verificato, installato e configurato a cura del settore elaborazione dati o di personale interno/esterno incaricato dal settore elaborazione dati.
3. L'utente sarà responsabile del funzionamento del software, della sua manutenzione e della integrità degli archivi gestiti.

## **Articolo 18 - Utilizzo dei supporti magnetici o ottici**

1. Tutti i supporti magnetici o ottici, contenenti dati sensibili, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato.
2. Tutti gli utenti devono porre particolare attenzione ai supporti di origine esterna adottando tutti gli accorgimenti finalizzati a prevenire l'esecuzione di programmi non autorizzati.
3. Tutti i supporti magnetici o ottici, contenenti dati sensibili, devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti.
4. La conservazione dei supporti avviene fino alla cessazione degli obblighi o delle necessità di custodia e sono custoditi in luogo sicuro ed inaccessibile. È il Dirigente del SIC che, su richiesta del dirigente competente, disporrà che i supporti magnetici contenenti le copie di tutti gli archivi siano utilizzabili per il ripristino o il recupero di archivi andati persi o danneggiati.

5. Gli utenti devono successivamente adottare tutti gli accorgimenti necessari per rendere inintelligibile e non ricostruibile tecnicamente i dati contenuti nei supporti, ovvero distruggere fisicamente tali supporti. La distruzione dei supporti si rende necessaria per impedire che essi vengano acceduti da persone non autorizzate al trattamento.



## **CAPO III**

### **Criteria di utilizzo delle apparecchiature telefoniche**

\* \* \* \* \*

#### **Articolo 19 - Utilizzo dei servizi e degli apparecchi telefonici**

1. Fermo restando il rispetto dei principi e dei doveri di cui all'art. 3, l'utilizzo delle utenze telefoniche di servizio per scopi personali è consentito solo in caso di urgenza, a fronte di occasionali ed improrogabili esigenze private.
2. Al fine di garantire un corretto utilizzo dei servizi di telefonia il Comune predispone, ove tecnicamente possibile, adeguate profilazioni che consentano l'effettuazione o meno delle diverse tipologie di chiamata (es. chiamate internazionali).
3. Il Comune, per finalità di gestione contabile, procede alla registrazione e alla conservazione, per il tempo strettamente necessario, dei tabulati del traffico effettuato. Per motivi di privacy le ultime tre cifre delle numerazioni sono oscurate.

#### **Articolo 20 - Disposizioni aggiuntive per la telefonia mobile**

1. E' fatto assoluto divieto di cessione ai terzi degli apparecchi e delle SIM.
2. Se le condizioni tecniche lo consentono, i cellulari di servizio assegnati agli utenti devono risultare attivi e raggiungibili quando essi sono in attività di servizio.
3. Il traffico telefonico per ragioni di servizio deve essere attestato dal dirigente responsabile dell'area assegnataria degli apparecchi di telefonia mobile, contestualmente alla consuntivazione periodica ivi prevista.

## CAPO IV

### Gestione delle comunicazioni telematiche

\* \* \* \* \*

#### Articolo 21 - Utilizzo di Internet

1. L'utilizzo di Internet deve essere limitato a scopi inerenti l'attività lavorativa.
2. L'amministrazione si riserva di applicare profili di navigazione personalizzati per aree o servizi, a seconda dell'attività professionale svolta. Attraverso tale profilazione, saranno consentite le attività di accesso, navigazione, registrazione a siti, scaricamento (download), ascolto e visione di file audio/ video in modo personalizzato e correlato con la propria attività lavorativa (c.d. "white list").
3. Ferme restando le modalità di utilizzo degli strumenti informatici di cui all'art. 9, durante l'espletamento della propria attività lavorativa, i dipendenti devono attenersi alle seguenti istruzioni e raccomandazioni:
  - a. non accedere ed evitare ogni forma di registrazione a siti Internet non attinenti allo svolgimento delle mansioni assegnate; in particolare è in ogni caso vietato accedere a siti i cui contenuti non siano adeguati alla serietà ed al decoro richiesti nei luoghi di lavoro.
  - b. è vietata la consultazione delle banche dati a pagamento (ad esempio, SISTER, SIATEL, ecc...) per finalità non pertinenti ai propri doveri d'ufficio, pur essendo autorizzati all'accesso.
  - c. non è consentita l'effettuazione di ogni genere di transazione finanziaria non rientrante nei compiti istituzionali tramite internet, con particolare riguardo a acquisti on-line e simili.
  - d. è facoltà dell'Amministrazione disporre controlli a campione sui siti web visitati. L'accesso ai dati di connessione, che comprendono data e ora della connessione, indirizzo IP di mittente e destinatario e volume complessivo dei dati trasmessi, è limitato all'amministratore di sistema, il quale è tenuto al rispetto delle norme in materia di protezione dei dati. I dati di connessione sono utilizzati esclusivamente per la ricerca di eventuali errori, per garantire la sicurezza del sistema, per verificare eventuali abusi.
  - e. non è permessa la partecipazione, per motivi non professionali a forum, l'utilizzo di chat line, di bacheche elettroniche, social network (ad esempio, Facebook e similari).
  - f. non è consentito scambiare materiale protetto dalla normativa vigente in tema di tutela del diritto d'autore e utilizzare sistemi di scambio dati/informazioni con tecnologie "peer to peer".
4. L'Amministrazione si riserva di applicare delle restrizioni ("Black list") alla navigazione sui siti internet ritenuti non opportuni per lo svolgimento delle proprie attività lavorative.

5. Il servizio è sottoposto a monitoraggio.
6. Il servizio può essere assoggettato a dei limiti dimensionali che possono essere variabili a seconda del profilo assegnato:
  - Limite temporale - Una volta raggiunta la scadenza temporale l'account verrà disattivato.
  - Fascia oraria di accesso - Fuori dalla fascia oraria assegnata non sarà possibile utilizzare il servizio.
  - Budget di minuti su base giornaliera/settimanale/mensile - Una volta raggiunto tale limite non sarà più possibile utilizzare il servizio.
  - Budget di banda occupata per la trasmissione/ricezione su base giornaliera/settimanale/mensile - Banda massima che il servizio potrà allocare sulla banda complessivamente disponibile.
  - Budget di Megabyte impiegati per la trasmissione/ricezione su base giornaliera/settimanale/mensile. Una volta raggiunto tale limite non sarà più possibile utilizzare il servizio.
7. Nel rispetto dei principi e doveri stabiliti nel codice di comportamento di cui all'art. 53 della L.R. 23 ottobre 1995, n°45, fermi restando i meccanismi di registrazione e i divieti di utilizzo di cui sopra, gli utenti possono utilizzare la rete internet per il tempo strettamente necessario ad assolvere incombenze amministrative e burocratiche di natura personale (adempimenti "on line" nei confronti di pubbliche amministrazioni, servizi pubblici, istituti bancari o assicurativi) senza allontanarsi dal luogo di lavoro.

## **Articolo 22 - Gestione e utilizzo della posta elettronica**

1. Ad ogni ufficio del Comune viene assegnata una casella di posta elettronica definita "casella di posta elettronica dell'ufficio o istituzionale" in ordine alla quale il Dirigente di riferimento individua un responsabile della gestione che deve assicurare quotidianamente la lettura e l'evasione delle e-mail ricevute. La "casella di posta elettronica dell'ufficio o istituzionale" potrà essere condivisa tra più addetti individuati dal Dirigente di riferimento, alcuni solo in lettura ed altri anche in lettura/scrittura.
2. In caso di assenze dal lavoro il Dirigente responsabile della gestione della "casella di posta elettronica dell'ufficio o istituzionale" deve delegare un altro lavoratore a verificare il contenuto dei messaggi della casella per garantire la continuità del servizio.
3. La posta elettronica è un mezzo di comunicazione messo a disposizione del dipendente esclusivamente per consentirgli lo svolgimento della propria attività lavorativa, con riferimento sia alla "casella di posta elettronica dell'ufficio o istituzionale", sia alla "casella di posta elettronica individuale".
4. In ogni caso non è consentito:
  - a. utilizzare tecniche di "mail spamming" (invio massiccio di comunicazioni);
  - b. utilizzare il servizio di posta elettronica per inoltrare "catene di Sant'Antonio", appelli e petizioni, giochi, scherzi e barzellette, ecc.;

- c. trasmettere, con dolo, virus, worms, Trojan o altro codice maligno, finalizzati ad arrecare danni e malfunzionamenti ai sistemi informatici.
5. Nel rispetto dei principi e doveri stabiliti nel Codice di comportamento di cui all'art. 3, comma 3, l'uso da parte dell'utente del servizio di posta elettronica a fini privati deve essere limitato ai meri casi di urgenza.
  6. La gestione delle caselle di e-mail avviene in modo centralizzato su server. L'accesso a tali caselle avviene preferibilmente mediante l'utilizzo della intranet (posta web). In caso di esigenze particolari di amministratori, dirigenti, funzionari, dipendenti assunti a tempo indeterminato, determinato e collaboratori esterni è possibile prevedere, previa autorizzazione da parte del Dirigente competente di concerto con il Servizio Sistemi Informativi Comunali, l'installazione di specifici programmi di gestione di posta elettronica .
  7. Ai fini di cui ai precedenti punti del presente articolo, non è consentita l'installazione di client di posta elettronica in locale (es. Microsoft Outlook).
  8. Al fine di garantire la continuità dell'attività lavorativa, in caso di assenza programmata e prolungata (ad es. per ferie), gli utenti sono tenuti ad utilizzare un'apposita funzionalità di sistema che invia automaticamente al mittente un messaggio di risposta, avvisando dell'assenza del destinatario e indicando eventuali modalità per contattare la struttura.
  9. In caso di assenze non programmate (es. per malattia), qualora l'utente non possa attivare la predetta procedura, se necessario il dirigente ne richiede formalmente l'attivazione all'amministratore di sistema.
  10. La nomenclatura delle caselle di posta elettronica adottata dal Comune di Gaeta è formalizzata nell'allegato "A" del Presente documento.
  11. In caso di cessazione del rapporto di lavoro, l'indirizzo di "casella di posta elettronica individuale" dell'interessato verrà immediatamente dismesso, come già stabilito al punto 6 dell'articolo 5 del presente regolamento.

## **CAPO V**

### **Assistenza e servizi**

\* \* \* \* \*

#### **Articolo 23 - Approvvigionamenti SIC e dotazioni**

1. Attivazione dell'e-procurement<sup>1</sup> per tutti gli approvvigionamenti di hardware e software, materiali di consumo. Sarà l'ufficio del Dirigente del SIC attraverso l'istituzione di una centrale unica d'acquisto, il quale, una volta pervenuta la richiesta inoltrata dall'ufficio richiedente, si attiva per verificare le necessità del richiedente ed attiva le necessarie procedure per l'eventuale approvvigionamento di materiale, nel rispetto delle norme per gli acquisti vigenti presso l'Ente e della normativa nazionale, utilizzando strumenti di acquisti online proposti dalla CONSIP. Per rendere veloce e trasparente l'attività, l'ufficio unico degli acquisti attiverà per tutte le necessità le RDO utilizzando il portale per gli acquisti on-line per la pubblica amministrazione [www.acquistiinretepa.it](http://www.acquistiinretepa.it).
2. Le procedure per gli approvvigionamenti si ispirano a principi di economicità, efficienza e funzionalità, perseguendo la standardizzazione dell'hardware e del software, nelle caratteristiche, marche, modelli, standard di qualità, ecc...

#### **Articolo 24 - Manutenzione SIC e dotazioni**

1. Il dirigente del SIC si occupa della manutenzione dell'hardware e del software esistenti nell'Ente, avvalendosi se necessario di fornitori esterni, e secondo le disposizioni contenute nel contratto di affidamento in essere il dirigente del SIC autorizza i relativi contratti di manutenzione ed assistenza, coordinando gli eventuali interventi e verificandone l'esatta applicazione, nel rispetto della normativa vigente. Le procedure per la manutenzione si ispirano a principi di economicità, efficienza e funzionalità. Il dirigente del SIC viene nominato dal Sindaco e deve riferire al Sindaco (titolare) sull'andamento e sulla produttività del sistema informativo comunale.

#### **Articolo 25 - Procedure operative**

1. Le procedure operative per le richieste di assistenza/servizi di cui al successivo comma 2 sono regolate da apposita procedura di gestione delle richieste (Service desk). Le richieste di assistenza dovranno pervenire per e-mail o per fax e dovranno contenere il guasto riscontrato, il nominativo richiedente, l'ufficio di appartenenza;

---

<sup>1</sup> È un sistema di approvvigionamento di beni e servizi attraverso la rete, dove è il consumatore (P.A. o azienda) a ricevere sul proprio sito le offerte di chi vende. Questo processo di acquisto consente alla Pubblica Amministrazione di ridurre i costi e velocizzare i tempi, guadagnando in termini di efficienza. In altre parole l'e-procurement è lo strumento che consente di automatizzare completamente le procedure di acquisto di tutti i prodotti e servizi. Questi prodotti possono essere cancelleria, attrezzature d'ufficio, supporti informatici e ogni altro strumento utilizzato per il supporto dell'attività.

ogni intervento di assistenza dovrà essere documentato con foglio di lavoro contenente data ed ora di intervento, il guasto riscontrato e se l'intervento è risolutivo o no. Le richieste di assistenza telefonica sui software applicativi non richiedono alcuna documentazione. Tutte le richieste devono pervenire all'ufficio del dirigente del SIC o a mezzo e-mail o a mezzo fax.

2. Il Service desk istruisce le principali richieste di assistenza/servizio, ovvero:
  - richiesta di acquisto, sostituzione o spostamento di un personal computer, stampante, scanner e altre apparecchiature;
  - richiesta di abilitazione all'accesso alla rete Internet;
  - richiesta di creazione del profilo di posta elettronica e abilitazione all'accesso della casella di posta elettronica dell'ufficio;
  - richiesta di accesso alle informazioni presenti nelle cartelle condivise d'ufficio;
  - richiesta di creazione, modifica e cancellazione di un'utenza per l'accesso ai servizi della rete comunale;
  - prenotazione per il prestito di un apparato multimediale (personal computer e proiettore);
  - richiesta di installazione di un nuovo applicativo;
  - richiesta di abilitazione ai servizi erogati sulla Intranet comunale per l'accesso a banche dati esterne;
  - richiesta di abilitazione ai servizi erogati sulla Intranet comunale per l'accesso a banche dati interne;
  - richiesta di ripristino del personal computer, stampante o altro dispositivo fornito dall'ente;
  - richiesta di ripristino del funzionamento di software e programmi applicativi installati dall'ente.
  
3. Il Dirigente del SIC dispone l'utilizzo delle risorse hardware e, sentito l'amministratore del sistema, dispone l'allocatione dei software applicativi che andranno tutti installati sull'unico server di cui il Comune si doterà.

## **CAPO VI Formazione**

\* \* \* \* \*

### **Articolo 26 - Formazione e Aggiornamento**

1. Il Comune di Gaeta promuove, all'interno del piano annuale della formazione, l'aggiornamento e la formazione dei propri dipendenti in merito al corretto utilizzo delle strumentazioni informatiche e delle apparecchiature telefoniche.

## **CAPO VII**

### **Modalità di controllo da parte del Comune**

\* \* \* \* \*

#### **Articolo 27 - Controlli, responsabilità e sanzioni**

1. L'Amministrazione si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici, della posta elettronica, di internet e delle apparecchiature telefoniche, nel rispetto delle normative vigenti e del presente regolamento.
2. Per esigenze organizzative, produttive e di sicurezza l'Amministrazione può avvalersi di strumenti che consentono un controllo a distanza di tipo generalizzato, indiretto e anonimo, relativo all'intera struttura amministrativa, ad aree, servizi o gruppi di utenti. Qualora - durante un controllo generalizzato - vengano rilevate anomalie nell'utilizzo degli strumenti informatici e telefonici, l'Amministrazione procede preliminarmente all'invio di un avviso generalizzato relativo all'uso improprio riscontrato, con l'invito ad attenersi scrupolosamente al presente regolamento e alla normativa vigente, e si riserva la facoltà di svolgere successive azioni mirate alla verifica del corretto utilizzo.
3. Qualsiasi utilizzo del sistema informativo dell'ente non conforme alle disposizioni del presente regolamento e/o alle leggi vigenti è ad esclusiva responsabilità dell'utente.
4. Nei casi in cui le figure di cui all'art. 5 accertino violazione del regolamento, è demandata ai rispettivi dirigenti l'applicazione dei necessari provvedimenti disciplinari, fermo restando l'obbligo di segnalare al titolare, al segretario generale ed alla competente autorità giudiziaria eventuali violazioni costituenti reato.
5. La violazione da parte degli utenti dei principi e delle norme contenute nel presente regolamento comporta l'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia, previo espletamento del procedimento disciplinare.
6. In coerenza con il punto 3 della deliberazione dell'Autorità Garante per la protezione dei dati personali 1° marzo 2007, n° 13, recante "Linee guida sull'utilizzo della posta elettronica ed internet", pubblicata nella GURI n° 58 del 10 marzo 2007, non si procede, al di là di quanto tecnicamente necessario per svolgere il servizio:
  - alla lettura e alla registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori;
  - alla riproduzione e alla eventuale memorizzazione sistematica delle pagine web visualizzate;
  - alla lettura e alla registrazione dei caratteri inseriti tramite tastiera o analogo dispositivo;
  - all'analisi di computer da remoto.



## **CAPO VIII INFORMATIVA**

\* \* \* \* \*

### **Articolo 28 - Informativa**

1. Ai sensi dell'art. 13 del Decreto Legislativo n° 196 del 30 giugno 2003 si comunica che:
  - l'Amministratore di sistema dovrà predisporre un sistema di "access log" come previsto dalla normativa;
  - il titolare dei dati di traffico è il Sindaco;
  - la presa visione e l'accettazione delle condizioni contenute nel presente Regolamento costituiscono l'informativa e l'esplicito consenso da parte dell'utente alla raccolta ed all'eventuale trattamento dei dati relativi al traffico.

## CAPO IX SCHEMI E MODULI

\* \* \* \* \*

### Articolo 29 - Validità degli schemi di moduli

L'amministratore di sistema ha la facoltà di modifica degli schemi di moduli per allinearli alle dotazioni del sistema informatico comunale.

### Articolo 30 - Presa visione ed accettazione del regolamento

#### Presenza visione ed accettazione del regolamento

Il sottoscritto/a \_\_\_\_\_

Nato/a \_\_\_\_\_

Residente \_\_\_\_\_ in via \_\_\_\_\_

Telefono \_\_\_\_\_ cod. fisc. \_\_\_\_\_

Dichiara di:

- aver preso visione ed accettare tutte le norme contenute nel regolamento d'uso del sistema Informativo del Comune di Gaeta;
- aver acquisito le informazioni di cui all'art. 13 del Decreto Legislativo 196 del 30 Giugno 2003;
- essere a conoscenza dei diritti dell'interessato di cui agli articoli 7, 8, 9, 10, del medesimo decreto.

Data \_\_\_\_\_ Firma \_\_\_\_\_

Allegati:

- Fotocopia documento di identità (Non necessario se l'utente è un dipendente comunale)
- Fotocopia dell'atto di affidamento dell'incarico o di attivazione del periodo di tirocinio.

### Articolo 31 - Richiesta di immagini tratte dal sistema di videosorveglianza

Al Sig. Sindaco del Comune di Gaeta

Il sottoscritto \_\_\_\_\_<sup>2</sup> appartenente a \_\_\_\_\_<sup>3</sup> estremi del documento di riconoscimento \_\_\_\_\_

a seguito dell'evento \_\_\_\_\_<sup>4</sup> per urgenti indagini di P.G. si prega di voler fare esaminare ed estrapolare su supporto ottico copia dei filmati relativi alle seguenti telecamere di sorveglianza comunali :

<sup>2</sup> Grado, cognome, nome

<sup>3</sup> Arma, comando, reparto, ufficio

<sup>4</sup> Indicare sommariamente l'evento, fornendo l'indirizzo presunto in cui è avvenuto il fatto

Telecamera \_\_\_\_\_ Indirizzo \_\_\_\_\_ Data Ora inizio \_\_\_\_\_ Ora fine \_\_\_\_\_  
Il richiedente \_\_\_\_\_ Data \_\_\_\_\_

Ricevuta

Si forniscono n° \_\_\_\_\_ supporti ottici \_\_\_\_\_ contenenti le immagini richieste.

Data \_\_\_\_\_ L'incaricato \_\_\_\_\_

Documento da conservare in duplice copia :

- comando di polizia municipale
- settore elaborazione dati

## **CAPO X NORME FINALI**

\* \* \* \* \*

### **Articolo 32 - Entrata in vigore**

Il presente regolamento entra in vigore decorsi 15 giorni dalla sua pubblicazione.

# Allegato “A”

## Linee guida per l’e-mail

### Premessa

Lo sviluppo del sistema informativo del Comune di Gaeta passa per la possibilità di comunicare con ogni dipendente e con ogni interlocutore esterno nella maniera più veloce possibile e con meno carta. A questo si deve aggiungere la necessità imposta dal sistema di documentazione elettronica che i comuni dovranno adottare a breve termine.

La soluzione passa per una adozione massiccia della posta elettronica con una casella per ogni dipendente, dirigente, sindaco, assessore e consigliere. Sono necessarie inoltre caselle di posta istituzionali per quelle comunicazioni che non sono “ad personam” e che riguardano i rapporti tra il cittadino e l’amministrazione o tra l’amministrazione e gli altri enti (uffici, commissioni, servizi, ecc.).

Un sistema di posta così eterogeneo e complesso deve presentarsi, almeno formalmente, all’occhio esterno in maniera omogenea e pertanto deve dotarsi di regole che lo rendano uniforme nel tempo. L’adozione di queste regole limita inoltre la necessità di richiedere autorizzazioni a creare caselle di posta elettronica di cui si è già regolamentata l’eventuale esistenza.

La scelta di adottare un sistema di posta elettronica basata sulla tecnologia web non solo rispetta quelle sono che le pregiudiziali del progetto “Comune On Line” ma pone le basi per comunicare da qualsiasi luogo ci si trovi raggiungendo quegli elementi di produttività e flessibilità necessari per dare una risposta in tempi rapidi al cittadino e per raggiungere quei livelli di alta affidabilità del mezzo informatico sempre invocata.

La tecnologia proposta ponendo come base la centralizzazione degli indirizzi aziendali e personali, il deposito dei messaggi e-mail e l’adozione di politiche di sicurezza, consente all’utente di vedere sempre salvaguardato il proprio lavoro a prescindere dal mezzo che sta utilizzando.

### ***Nomenclatura caselle e-mail***

Di seguito sono definite le modalità di costruzione delle caselle e-mail.

#### **Sindaco**

[nome.cognome@dominio](mailto:nome.cognome@dominio) oppure [sindaco@dominio](mailto:sindaco@dominio)

#### **Assessore**

[nome.cognome@dominio](mailto:nome.cognome@dominio)

Relativamente a questa figura è possibile che un assessore sia incaricato di seguire più aree, per cui è necessario utilizzare esclusivamente l’accoppiata “nome.cognome” per centralizzare le comunicazioni, viceversa dovrebbero esistere tante caselle e-mail quante sono le aree assegnategli.

#### **Consigliere**

[nome.cognome@dominio](mailto:nome.cognome@dominio)

La sintassi adottata è giustificata in quanto non necessariamente la propria figura è legata alla funzione della vita amministrativa.

#### **Area**

Non si considera interessante dedicare ad un’area specifica una casella di e-mail in quanto se l’obiettivo è solo di raggiungere con delle comunicazioni tutti gli appartenenti ad un’area questo è un obiettivo che si raggiunge con l’utilizzo delle liste di

distribuzione.

Per quanto riguarda le comunicazioni dal cittadino e dalle altre amministrazioni, esse sono rivolte sempre e comunque ai singoli servizi.

#### **Dirigente**

[nome.cognome@dominio](#)

Relativamente al dirigente si utilizza il proprio nominativo affinché l'eventuale cambio di responsabilità si tramuti in un cambio di comunicazione all'esterno anziché un trasferimento della propria casella di e-mail.

#### **Ufficio**

[ufficio.nomeufficio@dominio](#)

La sintassi adottata è prevista in funzione dell'interazione con altre amministrazioni e con la vita dell'ufficio stesso che prevede l'accesso di più utenti alla stessa casella di e-mail.

#### **Impiegato**

[nome.cognome@dominio](#)

La sintassi suggerita è unica in quanto identifica univocamente il dipendente consentendo una comunicazione elettronica preferenziale anche in funzione del sistema di gestione elettronica dei documenti e quindi del flusso di lavoro.

## Allegato “B”

### Glossario dei termini tecnici e informatici

<b>Account</b>	È la coppia nome utente e relativa password per l'accesso ad uno o più servizi rilasciata da una registrazione e consente l'accesso alla rete e/o ai servizi. Ad esempio, un account ci permette di entrare in Internet, un altro account ci serve per ricevere e spedire posta elettronica. Un account ci consente di accedere alle risorse di una rete locale, come server, file server, stampanti. Altri account servono per accedere a server e servizi vari .
<b>Antivirus</b>	Tipo di software che cerca e segnala gli eventuali programmi virus e cerca di rimediare ai danni che gli stessi virus hanno compiuto .
<b>Backup</b>	Copia di riserva di disco, di una parte del disco o di uno o più file.
<b>Black list</b>	Elenco di siti considerati non opportuni per l'espletamento delle funzioni lavorative dell'Amministrazione.
<b>Database</b>	(Base di Dati). Qualsiasi aggregato di dati organizzato in campo (colonne) e record (righe).
<b>Download</b>	Registrare sul proprio disco rigido un file richiamandolo, tramite modem o rete, da un computer, da un server o da un host (tramite Internet, rete locale o geografica).
<b>E-mail</b>	Electronic mail, posta elettronica. Scambio di messaggi e di file attraverso una rete locale o Internet. Avviene in tempo reale ed è indipendente dalla posizione fisica dei computer mittente e destinatario. I messaggi e file vengono conservati da un server che provvede ad inoltrarli al destinatario quando questo si collega.
<b>Firewall</b>	Insieme di software/hardware usato per filtrare i dati in scambio fra reti diverse, al fine di proteggere un server da attacchi pervenuti via rete locale o via Internet. Consente il passaggio solamente di determinati tipi di dati, da determinati terminali e determinati utenti.
<b>Freeware</b>	Software gratuito realizzato e distribuito da privati o piccole società, attraverso Internet o CD-ROM allegati a pubblicazioni in edicola.
<b>Hardware</b>	Letteralmente ferramenta, in informatica si intende l'insieme dei componenti (CPU, Hard Disk ecc.) che costituiscono un computer.
<b>Service Desk</b>	Risorsa informativa e di assistenza che prende in carico i problemi che sorgono nell'uso del sistema informativo comunale.
<b>Internet</b>	La madre di tutte le reti di computer. È l'insieme mondiale delle reti di computer interconnesse.
<b>Intranet</b>	La Intranet è una rete locale (Local Area Network), o un raggruppamento di reti locali, usata all'interno di una organizzazione per facilitare la comunicazione e l'accesso alle informazioni
<b>MP3 (MPEG-4)</b>	Tecnologia per la compressione/decompressione di file audio/video che consente di mantenere una perfetta fedeltà e qualità anche riducendo i file di ben 11 volte la grandezza originale.
<b>MPG (Motion Picture Experts Group)</b>	Stabilisce gli standard digitali per audio e video. E' in particolare lo standard di compressione utilizzato per codificare i video registrati su DVD.

<b>Password</b>	Parola che consente l'accesso di un utente ad una rete, ad un servizio telematico o ad un sito Internet. E' necessario digitarla esattamente (caratteri maiuscoli/minuscoli), assieme alla user-id.
<b>Quicktime</b>	Standard definito dalla Apple e utilizzato da tutti i computer per la riproduzione fedele dei filmati video.
<b>SIC</b>	Sistemi Informativi Comunali - Servizio che, nell'ambito dell'Amministrazione, si occupa di impostare, indirizzare e coordinare l'introduzione delle tecnologie informatiche nell'attività del Comune, ponendosi quale punto di riferimento tecnologico per la definizione delle strategie di evoluzione e innovazione dei Sistemi Informativi.
<b>Software</b>	Sono i programmi (professionali, ludici, video, musicali, raccolte di suoi ed immagini) per i computer.
<b>Streaming</b>	Con il termine streaming si intende un flusso di dati audio/video trasmessi da una sorgente a una o più destinazioni su Internet.
<b>Url filtering</b>	Sistema che permette di monitorare e filtrare la navigazione in Internet, bloccando l'accesso a particolari categorie di siti, al fine di limitare il rischio di utilizzo improprio della rete e la navigazione in siti non pertinenti o non compatibili con l'attività aziendale.
<b>User Id</b>	Nome utente
<b>Utente (User)</b>	Chiunque utilizzi un elaboratore collegato alla rete, sia che il collegamento avvenga in rete locale sia che si tratti di un accesso remoto.
<b>Virus</b>	Un programma creato per diffondersi da computer a computer, spesso danneggiando i dati e gli altri programmi registrati.
<b>White list</b>	Elenco di siti considerati opportuni per l'espletamento delle funzioni lavorative dell'Amministrazione.



---

---

Pareri favorevoli ai sensi dell'art.49 – 1° comma – del Dec. Lgs. 18/08/2000, n°267

Per la regolarità tecnica  
il Dirigente responsabile

f.to (Antonio Zangrillo Gallinaro)

Per la regolarità contabile  
il responsabile del Settore Finanziario

NON DOVUTO

---

---

Il sottoscritto Segretario Comunale, visti gli atti d'ufficio,

ATTESTA

Che il presente atto:

- ▶ Viene affisso in copia a questo Albo Pretorio, come prescritto dall'art.124, comma 1, del Dec. Lgs. 18/08/2000 n°267, per 15 giorni consecutivi a decorrere dal \_\_\_\_\_;
- ▶ Non è soggetto a controllo preventivo di legittimità ai sensi della Legge Costituzionale n°3/2001;
- ▶ È esecutivo perché dichiarato immediatamente eseguibile (art. 134 – comma 4 – del Dec. Lgs. 18/08/2000, n°267).

Li \_\_\_\_\_

\_\_\_\_\_

il Messo Comunale

F.to (Filippo Buonaugurio)

\_\_\_\_\_

il Segretario Generale

F.to (Avv. Celestina Labbadia)

---

---

Il sottoscritto Segretario Generale, visti gli atti d'ufficio

ATTESTA

Che il presente atto è divenuto esecutivo il \_\_\_\_\_

- ▶ perché decorso il decimo giorno della sua pubblicazione (art.134 – comma 3 – del Dec. Lgs. 18/08/2000 n°267).

Li \_\_\_\_\_

IL SEGRETARIO GENERALE

F.to (Avv. Celestina Labbadia)

---

---

COPIA CONFORME ALL'ORIGINALE, IN CARTA LIBERA PER USO AMMINISTRATIVO.

Addi \_\_\_\_\_

IL SEGRETARIO GENERALE

(Avv. Celestina Labbadia)

---

---